DVTEL INC.
65 Challenger Road
Ridgefield Park, NJ 07660

Quasar CM-3211 Series
Quasar CM-4221 Series
Mini-Dome Camera
User and Installation Guide

The contents of this guide may not be reproduced or reprinted in whole or in part without the express written permission of DVTEL, Inc.

Rev C June 2014

Table of Contents

1 Document Information vii

2 Overview 1

2.1 Features 2

2.2 Package Contents 3

2.3 Typical CM-3211/4221 Series Camera 4

3 Introduction to the CM-3211/4221 Series IP Mini-Dome Camera 5

3.1 CM-3211/4221 Indoor Camera Dimensions 5

3.2 CM-3211/4221-01 Outdoor Camera Dimensions 6

3.3 CM-3211/4221-10/10-I/11/11-I Motorized Camera Dimensions 6

3.4 Camera Connections 7

4 System Requirements 9

5 Installation 11

5.1 Indoor Installation 11

5.2 Outdoor Installation 11

5.3 Power and Ethernet Cable Connection 12

5.4 Initial Camera Configuration 12

5.5 Removing the Base Plate 14

5.6 Mounting Instructions 15

5.6.1 CM-3211/4221-10-I and CM-3211/4221-11-I Mounting Tips 15

5.6.2 Mounting the CM-3211/4221-00/10/10-I Indoor Camera 15

5.6.3 Mounting the CM-3211/4221-01/11/11-I Outdoor Camera 17

6 Using the DNA Utility to Search and Access the Camera 20

6.1 Introduction 20

6.2 Quick Start 20

6.3 Main Screen 21

6.4 Navigation Bar 21

6.5 Context Menu 22

6.6 Configuring Communication Settings on the Quasar Camera 22

6.7 Adjusting and Framing-Up the Camera View 26

7 Configuration and Operation 29

7.1 Browser-Based Viewer Introduction 29

7.2 Home Page 31

7.2.1 CM-3211/4221-00/01 Varifocal Camera Home Page 31

7.2.2 CM-3211/4221-10/10-I/11/11-I Motorized Camera Home Page 32

7.3 System-Related Settings 34

7.3.1 System 35

7.3.2 Security 36
7.3.3 Network 45
7.3.4 DDNS 51
7.3.5 Mail 52
7.3.6 FTP 53
7.3.7 HTTP 54
7.3.8 Application 55
7.3.9 Motion Detection 59
7.3.10 Network Failure Detection 63
7.3.11 Tampering 64
7.3.12 Storage Management 66
7.3.13 Recording 69
7.3.14 Schedule 70
7.3.15 File Location 71
7.3.16 View Information 72
7.3.17 Factory Default 75
7.3.18 Software Version 76
7.3.19 Software Upgrade 76
7.3.20 Maintenance 78
7.4 Video and Audio Streaming Settings 79
7.4.1 Video Format 79
7.4.2 Video Compression 90
7.4.3 Video OCX Protocol 91
7.4.4 Video Frame Rate 92
7.4.5 Video Mask 93
7.4.6 Audio 94
7.5 Camera-Related Settings 95
7.5.1 Exposure 96
7.5.2 White Balance 99
7.5.3 Picture Adjustment 100
7.5.4 Backlight 101
7.5.5 Digital Zoom 101
7.5.6 IR Function 102
7.5.7 WDR Function 103
7.5.8 Noise Reduction 104
7.5.9 TV System 105

7.6 Logout 106
8 Appendices 107
A.1. Technical Specifications 108
A.2. Device Search Software 111
A.2.1 Initial Camera Configuration 111
A.2.2 Searching and Accessing the Camera with Device Search 112
A.2.3 Configuring Communication Settings of a Quasar Camera 112
A.3. Internet Security Settings 116
A.4. Install UPnP Components 118
A.5. Deleting the Existing DCViewer 120
A.6. Deleting Temporary Internet Files 121
A.7. Connecting Leads to a Spring Clamp Terminal Block 122
A.8. Mounting Accessories 123
Contacting DVTEL 126

List of Figures

Figure 1: Package Contents....3
Figure 2: Typical CM-3211/4221-xx Camera with Motorized Lens....4
Figure 3: CM-3211/4221-00 Varifocal Indoor Camera Dimensions....5
Figure 4: CM-3211/4221-01 Varifocal Outdoor Camera Dimensions....6
Figure 5: CM-3211/4221-10 Motorized Indoor Camera Dimensions....6
Figure 6: CM-3211/4221 Camera Input/Output Connections....7
Figure 7: Discovered IP Devices....13
Figure 8: Network Setup Dialog Box....13
Figure 9: Inner Cover Removal....14
Figure 10: Releasing the Module....14
Figure 11: Removing the Camera Module from the Base Plate....14
Figure 12: Base Plate Used as a Template to Mark Drilling Locations....15
Figure 13: Threading Wiring through the Base Plate....16
Figure 14: Base Plate Used as a Template to Mark Drilling Locations....17
Figure 15: Top and Side Cable Entry Openings to Dome....18
Figure 16: Replacing Camera Module onto Base Plate....18
Figure 17: DNA Main Screen....21
Figure 18: Context Menu....22
Figure 19: Windows Firewall Screen....23
Figure 20: Discovered IP Devices....23
Figure 21: DNA Assign IP – Use DHCP Dialog Box....23
Figure 22: DNA Assign IP – Static IP Dialog Box....24
Figure 23: Installing the ActiveX Control....25
Figure 24: Security Window....25
Figure 25: CM-3211/4221 Camera – Pan, Rotate and Tilt Angles....26
Figure 26: Quasar Browser-Based User Interface....29
Figure 27: Home Page Function Buttons – for Varifocal Cameras....31
Figure 28: Home Page Function Buttons – for Cameras with Motorized Lens....32
Figure 29: Home Page – Step Range Drop-Down Menu....33
Figure 30: System Screen....34
Figure 31: System Configuration – Security....36
Figure 32: Security Screen....37
Figure 33: Editing Password and Privileges....38
Figure 34: Modifying Account Authority....38
Figure 35: HTTPS Screen....39
Figure 36: HTTPS Screen – Create Self-Signed Certificate....39
Figure 37: HTTPS Screen – Install Signed Certificate....40
Figure 38: HTTPS Screen – Upload Signed Certificate....40
Figure 39: Example of Self-Signed Certificate....41
Figure 40: Self-Signed Certificate – Details....41
Figure 41: IP Filter Screen....42
Figure 42: IEEE 802.1X/EAP-TLS Screen....43
Figure 43: Network Screen....45
Figure 44: QoS Screen....47
Figure 45: SNMP Settings Screen....48
Figure 46: UPnP Screen....50
Figure 47: Direct Access to Camera with UPnP Enabled....50
Figure 48: DDNS Screen....51
Figure 49: Mail Screen – SMTP....52
Figure 50: FTP Screen....53
Figure 51: HTTP Screen....54
Figure 52: Application Screen....55
Figure 53: Application – Record Stream to SD Card....56
Figure 54: Application – Upload Image by FTP....57
Figure 55: Application – Upload Image by E-Mail....57
Figure 56: Application – Send HTTP Notification....58
Figure 57: Motion Detection Screen....59
Figure 58: Motion Detection Screen – with Schedule Drop-Down Menu....60
Figure 59: Network Failure Detection Screen....63

Figure 60: Tampering Alarm Screen 64
Figure 61: Storage Management Screen 67
Figure 62: Video File Recording List 68
Figure 63: Selected File Window 68
Figure 64: Recording Screen 69
Figure 65: Schedule Screen 70
Figure 66: File Location Screen 71
Figure 67: System Log Screen 72
Figure 68: User Information Screen 73
Figure 69: User Information – Privileges Screen 73
Figure 70: Parameter List Screen 74
Figure 71: Factory Default Screen 75
Figure 72: Partial Restore Screen 75
Figure 73: Software Version Screen 76
Figure 74: Upgrade Screen 76
Figure 75: Software Upgrade – In Process 77
Figure 76: Maintenance Screen 78
Figure 77: File Download Screen 78
Figure 78: Video Format Screen 80
Figure 79: Video Rotate Type Screen 88
Figure 80: View-1 (Source) 89
Figure 81: View-2 Image Rotated Vertically (Reversed) 89
Figure 82: Video Compression Screen 90
Figure 83: Video OCX Protocol Screen 91
Figure 84: Video Frame Rate Screen 92
Figure 85: Mask Screen 93
Figure 86: Audio Screen 94
Figure 87: Camera Settings Screen 95
Figure 88: Camera Settings Screen – Exposure 96
Figure 89: Camera Settings Screen – White Balance 99
Figure 90: Camera Settings Screen – Picture Adjustment 100
Figure 91: Camera Settings Screen – Backlight 101
Figure 92: Camera Settings Screen – Digital Zoom 101
Figure 93: Camera Settings Screen – IR Function 103
Figure 94: Camera Settings Screen – WDR Function 103
Figure 95: Camera Settings Screen – Noise Reduction 104
Figure 96: Camera Settings Screen – TV System 105
Figure 97: Login Message 106
Figure 98: Login Window 106
Figure 99: Device Search Application 111
Figure 100: Windows Security Alert 113
Figure 101: Device Search Application – Select Browse 114
Figure 102: Device Search Application – Select Install ActiveX Control 114
Figure 103: Security Warning Window 114
Figure 104: Command Bar Toolbar – Select Internet Options 116
Figure 105: Internet Options Screen 116
Figure 106: Command Bar Toolbar – Internet Options 117
Figure 107: Schedule Screen 117
Figure 108: Spring Clamp Terminal Block 122
Figure 109: Connecting a Wire to a Terminal Block 122

Revision History

Version	Date	Author	Comments
A	October 2013	Jonathan Herman Alan Singer	First release. Combined CM-3211 and CM-4221 UIGs into one document. Adding instructions to set a schedule for motion detection, network failure detection, and for the tampering alarm. Added section 7.4.1.8 (GOV Settings). Added Gain Control to Manual Mode in section 7.5.1 (Exposure). General editing.
B	Nov. 27, 2013	Alan Singer	Updated look and feel.
C	June 19, 2014	Alan Singer	Updated look and feel. Added Revision History. Updated images in section 6.

1 Document Information

Document Scope and Purpose

The purpose of this document is to provide instructions and installation procedures for physically connecting the Quasar camera. After completing the physical installation, additional setup and configurations may be required before video analysis and detection can commence.

Note:
This document is intended for use by technical users who have a basic understanding of CCTV camera/video equipment and LAN/WAN network connections.

Warning:
Installation must follow safety, standards, and electrical codes as well as the laws that apply where the units are being installed.

Proprietary Rights and Non-Disclosure

This manual is delivered subject to the following restrictions and conditions:

- This document contains proprietary information belonging to DVTEL, Inc. This information is supplied solely for the purpose of assisting explicitly the licensee of the DVTEL units.
- No part of this document contents may be used for any other purpose, disclosed to any third party or reproduced by any means, electronic or mechanical, without the express prior written permission of DVTEL, Inc.

Trademarks and Copyrights

This manual and its contents herein are owned by DVTEL, Inc. All rights reserved.

DVTEL, the DVTEL logo, Quasar CM-3211/4221 are trademarks of DVTEL, Inc.

Products and trademarks mentioned herein are for identification purposes only and may be registered trademarks of their respective companies.

DVTEL, Inc. makes no representations whatsoever about any other products or trademarks mentioned in the manual.

© DVTEL, Inc. 2014. All rights reserved.

Disclaimer

Users of DVTEL products accept full responsibility for ensuring the suitability and considering the role of the product detection capabilities and their limitation as they apply to their unique site requirements.

DVTEL, Inc. and its agents make no guarantees or warranties to the suitability for the users' intended use. DVTEL, Inc. accepts no responsibility for improper use or incomplete security and safety measures.

Failure in part or in whole of the installer, owner, or user in any way to follow the prescribed procedures or to heed WARNINGS and CAUTIONS shall absolve DVTEL, Inc. and its agents from any resulting liability.

Specifications and information in this guide are subject to change without notice.

Document Conventions

WARNING and **CAUTION** notes are distributed throughout this document, whenever applicable, to alert you of potentially hazardous situations. These may be hazards associated with a task or a procedure you are carrying out or are about to carry out.

The following document conventions are used throughout this manual:

A **Warning** is a precautionary message that indicates a procedure or condition where there are potential hazards of personal injury or death.

A **Caution** is a precautionary message that indicates a procedure or condition where there are potential hazards of permanent damage to the equipment and or loss of data.

A **Note** is useful information to prevent problems, help with successful installation, or to provide additional understanding of the products and installation.

A **Tip** is information and best practices that are useful or provide some benefit for installation and use of DVTEL products.

General Cautions and Warnings

This section contains information that indicates a procedure or condition where there are potential hazards. These may be hazards associated with a task or procedure a user is carrying out or about to carry out. WARNINGS and CAUTIONS are distributed throughout this document, whenever applicable, to alert the user of potentially hazardous situations.

SAVE ALL SAFETY AND OPERATING INSTRUCTIONS FOR FUTURE USE.

Although the unit is designed and manufactured in compliance with all applicable safety standards, certain hazards are present during the installation of this equipment.

To help ensure safety and to help reduce risk of injury or damage, observe the following:

Warning:

1. The camera covers is an essential part of the product. Do not open or remove it.
2. Never operate the camera without the cover in place. Operating the camera without the cover poses a risk of fire and shock hazards.
3. Do not disassemble the camera or remove screws. There are no user serviceable parts inside the unit.
4. Only qualified trained personnel should service and repair this equipment.
5. Observe local codes and laws and ensure that installation and operation are in accordance with fire, security and safety standards.

Electrical Safety Notice and Warnings

Warning:

1. Read the installation instructions before you connect the unit to a power source**.**
2. Electrical safety should always be observed. All electrical connections must be performed by a certified electrician.
3. Use the supplied power supply and protect against static electricity, ground faults and power surges.
4. The unit uses a three-wire power cord to make sure that the product is properly grounded when in use. This is a safety feature. If the intended power outlet does not support three prongs, one of which is a ground, contact an electrician to install the appropriate outlet. NEVER remove or otherwise attempt to bypass the ground pin of the power cord. Do not operate the unit in the absence of a suitably installed ground conductor**.**
5. If you use an extension cord with this system, make sure that the total ampere rating on the products plugged into the extension cord does not exceed the extension cord ampere rating.
6. To avoid possible shock hazards or damaging the unit, assure that the positive and negative of the power leads are properly connected to the terminal block connector before plugging it into the unit or turning on the power source.
7. In the following situations, the electric power should be turned off immediately and appropriate repairs, replacements or remedies should be taken if:
   - The power line is damaged, frayed or shows heavy wear.
   - The unit has been physically crushed or deformed.
   - The unit has been exposed to water.
   - The unit has been exposed to, or shows signs of damage from, fire, intense heat, heavy smoke, fumes, or vapors.
   - Electrical connections of the unit become abnormally hot or generate smoke.
   - The unit has been dropped, damaged or shows signs of loose internal parts.
   - The unit does not operate properly.

Caution:
To avoid damage from overheating or unit failure, assure that there is sufficient temperature regulation to support the unit's requirements (cooling/heating). Operating temperature should be kept in the range 0° to 50°C (32° to 122°F), with no more than 90% non-condensing humidity.

Minimizing EMI and RFI

When wires run for a significant distance in an electromagnetic field, electromagnetic interference (EMI) can occur. Strong EMI (e.g. lightning or radio transmitters) can destroy the units and can pose an electrical hazard by conducting power through lines and into the system. Poor quality or worn wiring can result in radio frequency interference (RFI). To minimize the effects of EMI and RFI, consult your reseller.

Site Preparation

There are several requirements that should be properly addressed prior to installation at the site. The following specifications are requirements for proper installation and operation of the unit:

- **Ambient Environment Conditions**: Avoid positioning the unit near heaters or heating system outputs. Avoid exposure to direct sunlight. Use proper maintenance to ensure that the unit is free from dust, dirt, smoke, particles, chemicals, smoke, water or water condensation, and exposure to EMI.
- **Accessibility**: The location used should allow easy access to unit connections and cables.
- **Safety**: Cables and electrical cords should be routed in a manner that prevents safety hazards, such as from tripping, wire fraying, overheating, etc. Ensure that nothing rests on the unit's cables or power cords.
- **Ample Air Circulation**: Leave enough space around the unit to allow free air circulation.
- **Cabling Considerations**: Units should be placed in locations that are optimal for the type of video cabling used between the unit and the cameras and external devices. Using a cable longer than the manufacturer's specifications for optimal video signal may result in degradation of color and video parameters.
- **Physical Security**: The unit provides threat detection for physical security systems. In order to ensure that the unit cannot be disabled or tampered with, the system should be installed with security measures regarding physical access by trusted and un-trusted parties.
- **Network Security**: The unit transmits over IP to security personnel for video surveillance. Proper network security measures should be in place to assure networks remain operating and free from malicious interference. The unit is intended for installation on the backbone of a trusted network.
- **Electrostatic Safeguards**: The unit as well as other equipment connected to it (relay outputs, alarm inputs, racks, carpeting, etc.) shall be properly grounded to prevent electrostatic discharge.

The physical installation of the unit is the first phase of making the unit operational in a security plan. The goal is to physically place the unit, connect it to other devices in the system, and to establish network connectivity.

2 Overview

The Quasar CM-3211 Series IP Mini-Dome Camera provides real-time, 720p, H.264 multi-streaming with the highest quality image. Its compact, sophisticated mechanical design and snap-in camera chassis facilitate easy installation. The CM-3211 series includes the following models (collectively referred to as CM-3211-xx):

- CM-3211-00 Indoor Camera with varifocal lens
- CM-3211-01 Outdoor Camera with varifocal lens
- CM-3211-10 Indoor Camera with motorized lens
- CM-3211-10-I Indoor Camera with motorized lens and infrared IR illuminator
- CM-3211-11 Outdoor Camera with motorized lens
- CM-3211-11-I Outdoor Camera with motorized lens and infrared IR illuminator

The Quasar CM-4221 Series IP Mini-Dome Camera provides real-time, 1080p, H.264 multi-streaming with the highest quality image. Its compact, sophisticated mechanical design and snap-in camera chassis facilitate easy installation. The CM-4221 series includes the following models (collectively referred to as CM-4221-xx):

- CM-4221-00 Indoor Camera with varifocal lens
- CM-4221-01 Outdoor Camera with varifocal lens
- CM-4221-10 Indoor Camera with motorized lens
- CM-4221-10-I Indoor Camera with motorized lens and infrared IR illuminator
- CM-4221-11 Outdoor Camera with motorized lens
- CM-4221-11-I Outdoor Camera with motorized lens and infrared IR illuminator

Caution:
If you are using DVTEL Latitude, we recommend that you configure the camera's settings via the AdminCenter. This is because the camera's web-based interface might be overwritten by Latitude settings. Refer to the Latitude online help for information regarding configuring camera settings.

2.1 Features

Following are key features of the CM-3211/4221 series cameras:

- H.264 and MJPEG compression
- HTTP streaming MJPEG
- Progressive scan CMOS sensor
- Edge motion detection
- Motion detection with region of interest masking
- Historical motion-detection levels detected/recorded at frame levels.
- Detection event driven alarms
- Alarm input driven events
- Relay output actions on alarm
- Built-in web application/web server
- FTP upload (up to two locations)
- Upload alarm images to FTP
- Dual HTTP notification server support (up to two servers)
- Send images on alarm to e-mail
- E-Mail SMTP alarm notification (up to two e-mails)
- MicroSD/SDHC recording support
- Record snapshots to SD card on alarm
- Sequential snapshot numbering
- SNMP v1/v2/v3 and SNMP traps
- Security IP restricted access allow/deny list
- UPnP support
- Electronic day/night (ICR)
- Analog video output
- BNC analog output
- Privacy masks
- WDR and ATW
- 3DNR image noise reduction
- ONVIF support
- RTSP support
- Supports PoE /12VDC/24VAC
- Multiple users
- Group permissions
- Per-user permissions
- Tampering detection and notification
- Two encoder streams available
- Low-lux mode and backlight compensation
- Vandal-proof IP66 enclosure (CM-3211/4221-01/11/11-I)
- Motorized lens (CM-3211/4221-10/11/11-I)
- Infrared LED illuminator (CM-3211/4221-10-I/11-I)

Note:
MJPEG is not supported by Latitude.

2.2 Package Contents

Before proceeding, please check that the box contains the items listed here. If any item is missing or has defects, do not install or operate the product and contact your dealer for assistance.

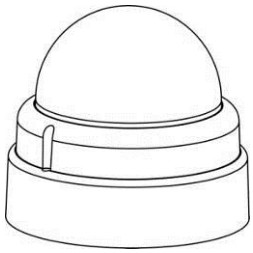
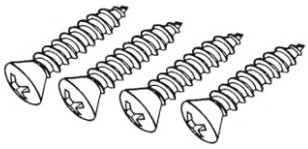
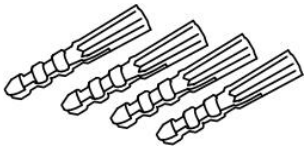
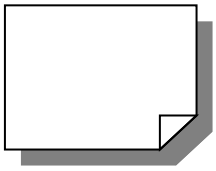
 Mini-Dome camera	(Torx wrench)	Rubber washers (×6)
 Self-tapping screws (×4) (See Note below)	 Plastic screw anchors (×4)	CD (Bundled software and documentation)
	 Quick-start guide	

Figure 1: Package Contents

Note:
The self-tapping screws are mainly for softer substrate/material installation such as wood. For other installation materials such as cement ceilings, it is necessary to pre-drill and use plastic anchors before fastening the supplied self-tapping screws into the wall.

2.3 Typical CM-3211/4221 Series Camera

The figure below shows a typical CM-3211/4221 series camera.

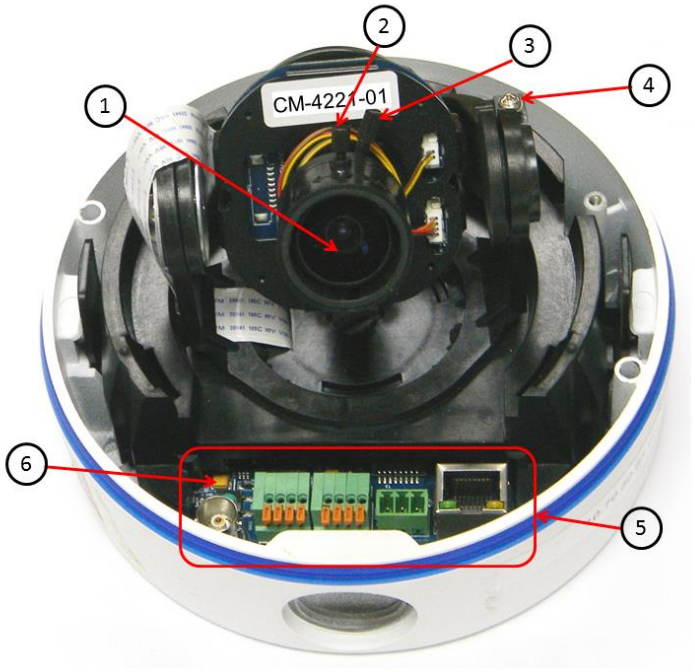


Figure 2: Typical CM-3211/4221-xx Camera with Motorized Lens

Table 1: CM-3211/4221 Camera Control Descriptions

Item	Designation	Description
1	Lens	Camera lens
2	Focus fixing knob	To set the focus, loosen and tighten by hand the adjustment knob until the optimum focus is obtained
3	Zoom fixing knob	To set the zoom, loosen and tighten by hand the adjustment knob until the optimum zoom is obtained
4	Tilt fixed screw	To set the tilt, loosen the screw, adjust the tilt angle and tighten screw
5	Input/output connections	Refer to Figure 6
6	Reset button	Restores the default setting

3 Introduction to the CM-3211/4221 Series IP Mini-Dome Camera

This chapter provides the camera dimensions for reference before installation. Each connector located inside the camera's housing is also identified. See Figure 6 and Table 2.

Related Links

- CM-3211/4221-00 Indoor Camera Dimensions
- CM-3211/4221-01 Outdoor Camera Dimensions
- CM-3211/4221-10/10-I/11/11-I Motorized Camera Dimensions
- Camera Connections
- Technical Specifications

3.1 CM-3211/4221 Indoor Camera Dimensions

The CM-3211/4221-00 IP Indoor Varifocal Mini-Dome Camera's dimensions are shown below.

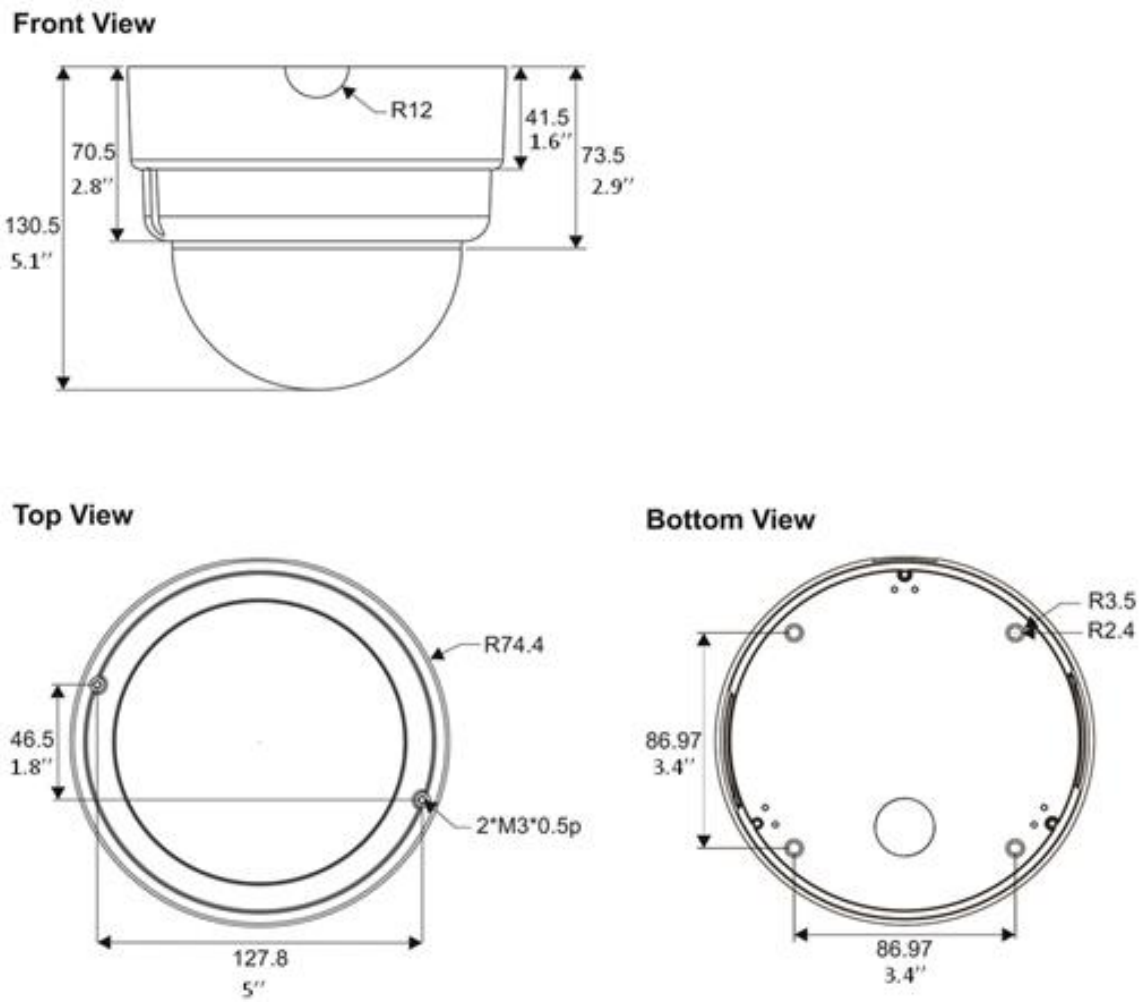


Figure 3: CM-3211/4221-00 Varifocal Indoor Camera Dimensions

3.2 CM-3211/4221-01 Outdoor Camera Dimensions

The CM-3211/4221-01 Varifocal IP Outdoor Mini-Dome Camera dimensions are shown below.

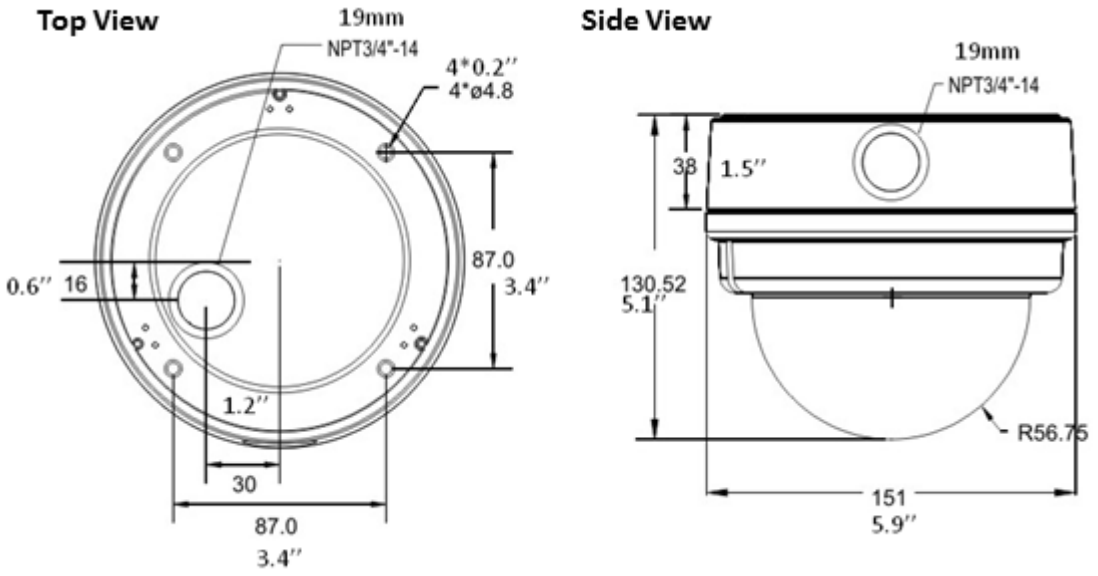


Figure 4: CM-3211/4221-01 Varifocal Outdoor Camera Dimensions

3.3 CM-3211/4221-10/10-I/11/11-I Motorized Camera Dimensions

The CM-3211/4221-10, CM-3211/4221-10-I, CM-3211/4221-11, and CM-3211/4221-11-I Indoor and Outdoor Motorized IP Mini-Dome Camera dimensions are shown below.

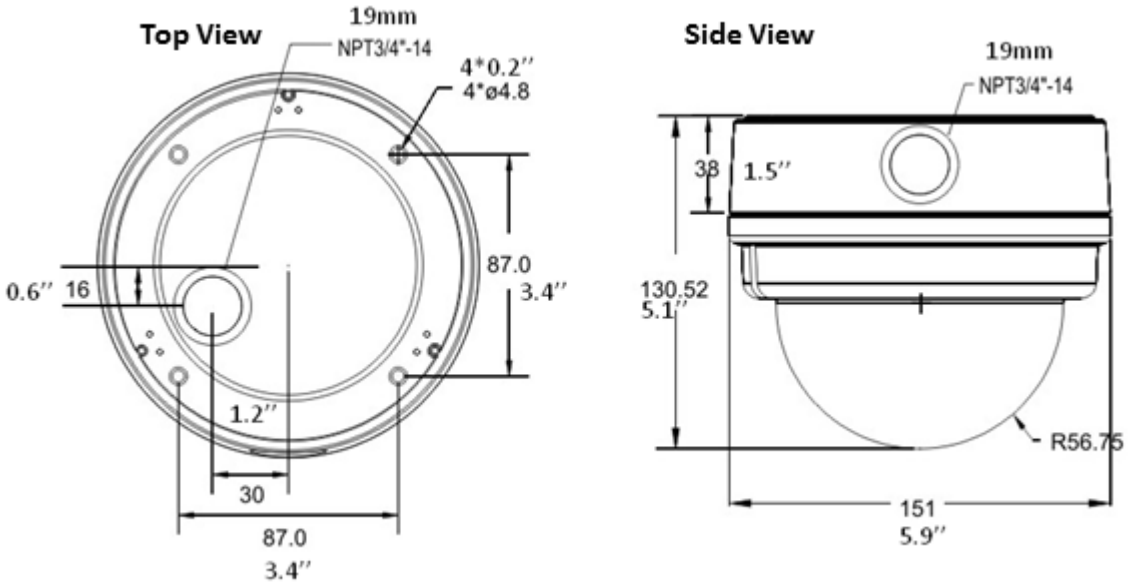


Figure 5: CM-3211/4221-10 Motorized Indoor Camera Dimensions

Related Link

- Technical Specifications

3.4 Camera Connections

Figure 6 shows the various connectors and Reset button contained within the housing of the CM-3211/4221-xx camera. The connectors, pin numbers and signal definitions related to each pin are listed in Table 2.

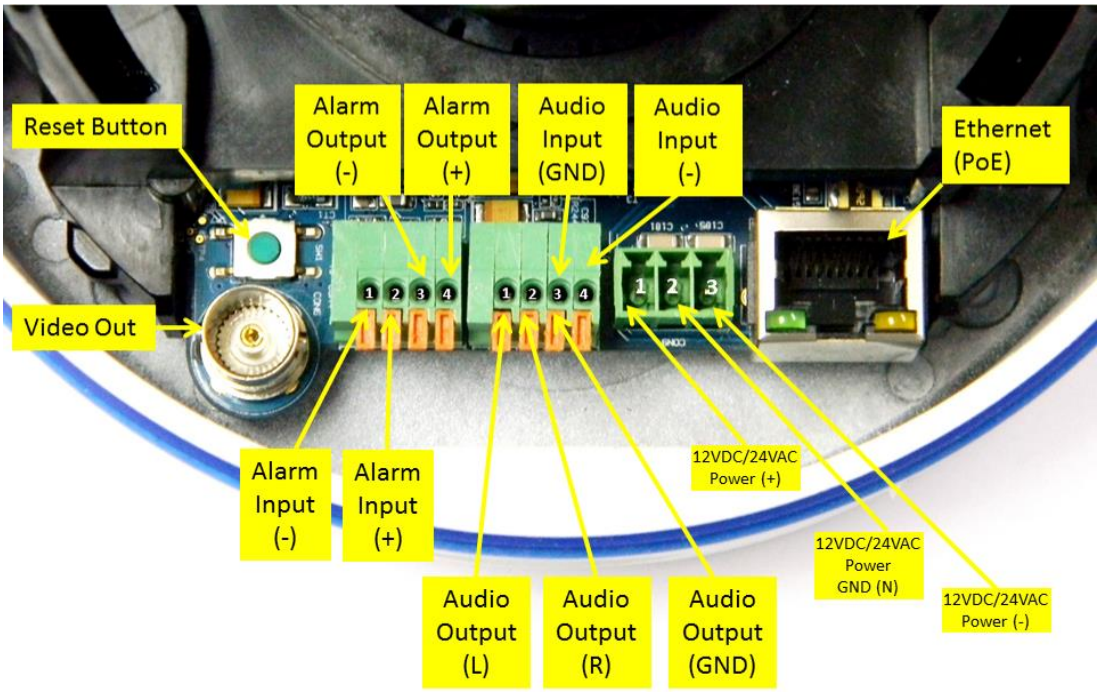


Figure 6: CM-3211/4221 Camera Input/Output Connections

Table 2: CM-3211/4221 Camera Connector Designations

Connector		Pin No.	Definition	Remarks
BNC		**N/A**	**Analog Video Output**	
Alarm I/O		1 2 3 4	GND (Input－) Input＋ Output－ Output＋	Alarm connection
Audio I/O		1 2 3 4	Output (L) Output (R) GND Input	Two-way audio transmission
Power	**12VDC**	1 2 3	Power Reserved GND	Power connection
	24VAC	1 2 3	Power-1 Earth GND Power-2	
RJ45		N/A	10/100 Mbps Ethernet/PoE	

Table 3: CM-3211/4221 Camera Reset

Switch	Pin No.	Definition	Remarks
Reset Button	N/A	Restores to factory default	

4 System Requirements

To access the camera via a web browser, ensure that your PC has the proper network connection and meets system requirements as described below.

Table 4: System Requirements

Item	Minimum System Requirement
Personal Computer	Intel® Pentium® M, 2.16 GHz or Intel® Core™2 Duo2.0 GHz 2GB RAM or more
Operating System	Windows, Windows XP, Windows 7
Web Browser	Microsoft Internet Explorer 7, 8, or 9
Network Card	10Base-T (10 Mbps) or 100Base-TX (100 Mbps) operation
Viewer	ActiveX control plug-in for Microsoft IE

5 Installation

Follow the instructions below for indoor and outdoor installation of the Quasar CM-3211/4221 series camera.

Related Links

- Indoor Installation
- Outdoor Installation
- Power and Ethernet Cable Connection
- Initial Camera Configuration
- Removing the Base Plate
- Mounting Instructions

5.1 Indoor Installation

Read the instructions provided in this chapter thoroughly before installing the CM-3211/4221-00, CM-3211/4221-10, or CM-3211/4221-10-I. Following are additional considerations for indoor installation:

- There must be a fuse or circuit breaker at the starting point of the electrical wiring infrastructure.
- For indoor installations, such as industrial applications, the camera must be protected from hostile external elements (e.g. corrosive environment, metallic dust, extreme temperatures, soot, moisture, over spray, etc.).
- Do not place the camera on or near radiators and heat sources.
- All electrical work must be performed in accordance with local regulatory requirements.

5.2 Outdoor Installation

Read the instructions provided in this chapter thoroughly before installing the CM-3211/4221-01, CM-3211/4221-11, or CM-3211/4221-11-I camera. Following are additional considerations for outdoor installation:

- For outside wiring installation, always use weatherproof equipment, such as boxes, receptacles, connectors, etc.
- For electrical wiring, use the properly rated sheathed cables for conditions to which the cable will be exposed (for example, moisture, heat, UV, physical requirements, etc.).
- Plan ahead to determine where to install infrastructure weatherproof equipment. Whenever possible, ground components to an outdoor ground.
- Use best security practices to design and maintain secured camera access, communications infrastructure, tamper-proof outdoor boxes, etc.
- All electrical work must be performed in accordance with local regulatory requirements.

5.3 Power and Ethernet Cable Connection

Power Connection

Make sure the camera's power cable is properly connected. Refer to Camera Connections. If using Power over Ethernet (PoE), make sure Power Sourcing Equipment (PSE) is available on the connected network. All electrical work must be performed in accordance with local regulatory requirements.

5.4 Initial Camera Configuration

To perform the initial camera configuration:

1. Unpack the camera. Rotate and remove the protective cover.

2. Remove the PE cloth sheet and lens cap. Attach the dome cover to the body.
3. Connect one end of the Cat 5 Ethernet cable to the Ethernet port of the camera and the RJ45 connector at other end to the Power Sourcing Equipment (PSE) device, such as a switch.
4. Verify that the RJ45 connector LEDs illuminate green (indicating a stable network connection) and flashing yellow (to indicate network activity).
5. Do one of the following:
   - Copy and run the dna.exe (see note below) from the included CD.

     Note:
     DNA is an enhanced software alternative to Device Search. Either of these programs may be used. They are supplied on the included CD.

   - From the Latitude Sidebar, run the Unified Configurator by selecting **Applications > Device Configuration Tool** and then, on the Unified Configurator screen, click **DVTEL HD Series**.

6. Mark the unit requiring IP assignment.

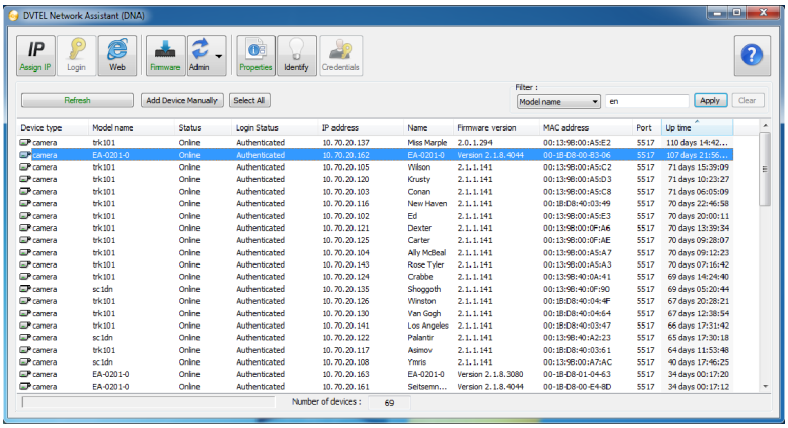


Figure 7: Discovered IP Devices

7. Right-click on the mouse and select the assigned IP or press the Assign IP button to open the DNA Assign IP screen.
8. In the dialog box that is displayed, enter values for the *IP Address, Gateway and Netmask*.
9. Click **Update** and wait for *OK* status to be displayed.

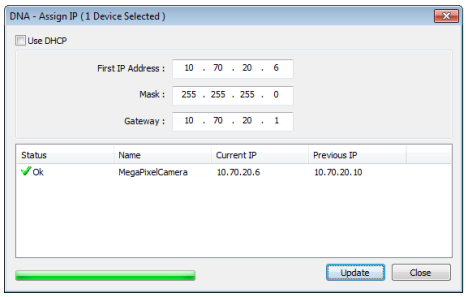


Figure 8: Network Setup Dialog Box

10. Disconnect the Ethernet cable. The camera is ready for deployment (mounting) in a site installation.

Note:
The camera can be connected to a PC for bench installation via an Ethernet cross-cable.

Note:
The camera default IP Address and the subnet mask IP Address are automatically supplied by the DHCP server.

Tip:
A camera setup adapter, such as Veracity Pinpoint, can be used to connect a laptop directly to the camera when using PoE.

5.5 Removing the Base Plate

To remove the base plate:

1. If you have not already removed the Mini-Dome cover, unscrew and remove it using the star-bit tool supplied with the camera.
2. Press the sides of the inner cover inward and remove the cover. See Figure 9.

Figure 9: Inner Cover Removal

3. Unscrew the module-fastening screw.

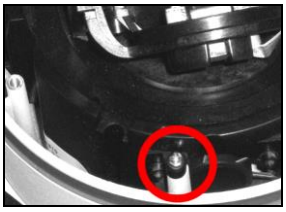


Figure 10: Releasing the Module

Caution:
The CM-3211/4221-x0 is an indoor camera and should be kept in a clean and dry indoor environment. Operating temperature should be maintained within a range of 10° to 50°C (-14° to 122°F). Operating humidity is 10% to 90% (non-condensing). The camera should be kept dry, free from water condensation, dust, dirt, and smoke.

4. Press in the camera module flanges to unsnap the camera module from the base plate.

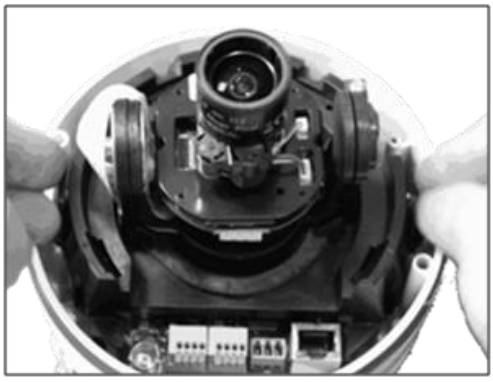


Figure 11: Removing the Camera Module from the Base Plate

5.6 Mounting Instructions

The following are mounting instructions for the CM-3211/4221 series cameras.

- CM-3211/4221-10-I and CM-3211/4221-11-I Mounting Tips
- Mounting the CM-3211/4221-00/10/10-I Indoor Camera
- Mounting the CM-3211/4221-01/11/11-I Outdoor Camera

5.6.1 CM-3211/4221-10-I and CM-3211/4221-11-I Mounting Tips

To eliminate IR reflection:

1. Clean the bubble from dirt and finger prints.
2. Make sure the bubble has no scratches.
3. Fasten the screw that secures the snap-in chassis in order to have the rubber sealed against the bubble.
4. Avoid aiming the IR where there are nearby objects closer than the scene of interest which might reflect back into the lens.

5.6.2 Mounting the CM-3211/4221-00/10/10-I Indoor Camera

1. Do one of the following:
   - For drilled wall or ceiling mounting:

     a) Use the base plate as a template, mark with a pointed pencil, the mounting surface through the plate holes where the four screw holes will need to be drilled (see Figure 12).

> **Caution:**
> Before marking and drilling the holes, ensure that the base plate alignment is oriented correctly so that the required camera field of view can be achieved when the system is assembled.

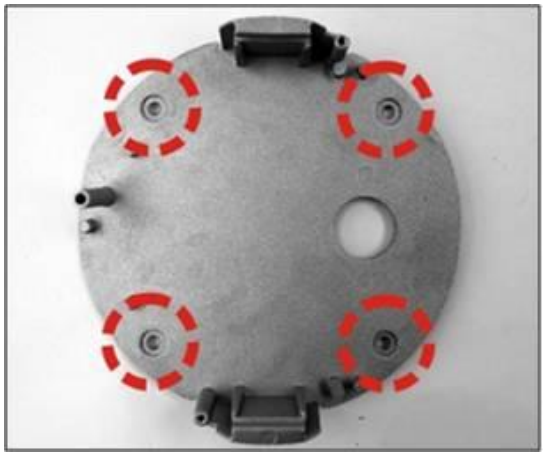


Figure 12: Base Plate Used as a Template to Mark Drilling Locations

b) In the marked locations, drill each hole using a drill-bit of a slightly smaller diameter than the supplied screw anchors (molly-plug anchor). You want to achieve a snug insertion so that the plug expansion holds firm after the screws are screwed in.

c) Fully insert the supplied anchors into drilled holes. You may need to tap them flush with the wall using a hammer.

- For installing on a 4S recessed electrical box:

a) Have a qualified installer (check your local electrical codes) rough-in the 4S recessed electrical box and run the wires and power (if not PoE) through the wall/conduits to the box location.

b) Ensure that the box is sufficiently sturdy (attach to the wall stud, ceiling joist, or reinforced surface as needed) to securely hold the weight of the camera.

- For bracket, pole and pendant installations, follow the hanging device installation instructions.

2. If running the cables through the back, thread the power and Ethernet cables and any other wires (such as a relay output, alarm input, audio in, or audio out) through the back wire entry. If you are not wiring from within the wall, you can run the wires through the slot on the side of the Mini-Dome. Punch out the half circle slot and run the wires through this slot.

Tip:
Even if you are not using alarm inputs and audio input/output at the time of installation, you may want to consider pre-wiring these connections for future use.

Note:
The power cable is not required if using PoE.

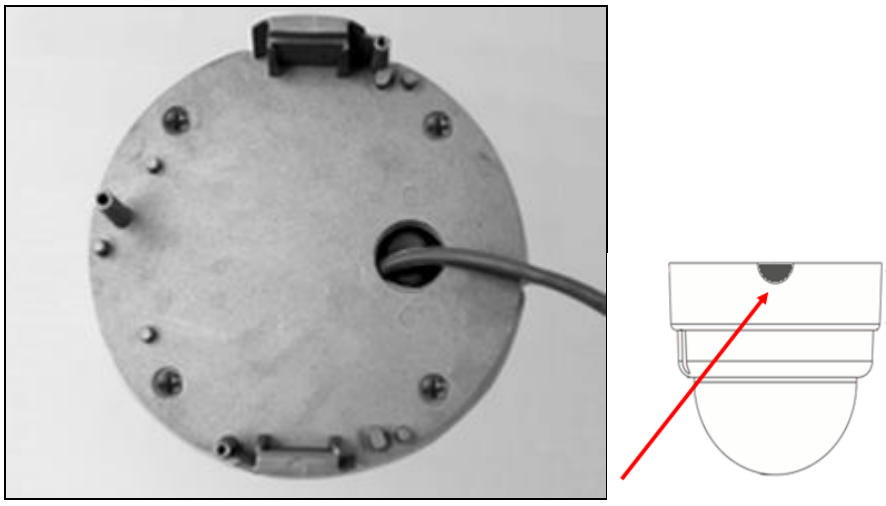


Figure 13: Threading Wiring through the Base Plate

3. Thread the wires through the base plate and screw it to the predrilled wall, ceiling, CM Series Mini-Dome Recessed Mount, CM Series Mini-Dome Corner Mount, or 4S electrical box. Check that the installation is not flimsy, will not wobble, and is flush with the mounting surface.

Tip:
Use shims for shoring up mounts on uneven surfaces.

4. Snap the camera module back on the base plate with the wiring threaded through the gap at the module base and then screw in the module-fastening screw.

5. Plug the Cat 5 cable into the camera's Ethernet port and, if needed, plug the power terminal block into the power terminals.
6. If applicable, wire the Alarm In, Alarm Out, Audio In, and Audio Out terminal blocks to external devices. See Figure 6: CM-3211/4221 Camera Input/Output Connections.
7. If needed, connect the other end of the Cat 5 cable to the network and turn on the power from the power supply.

Note:
Do not reassemble the camera's inner cover and Mini-Dome cover until after hardware configurations and lens adjustments are made.

5.6.3 Mounting the CM-3211/4221-01/11/11-I Outdoor Camera

1. Do one of the following:
   - For drilled wall or ceiling mounting:
     a) Use a pointed pencil and the base plate as a template to mark the mounting surface through the plate holes where the four screw holes will need to be drilled.

Caution:
Before marking and drilling the holes, ensure that the base plate alignment is oriented correctly so that the required camera field of view can be achieved when the system is assembled.

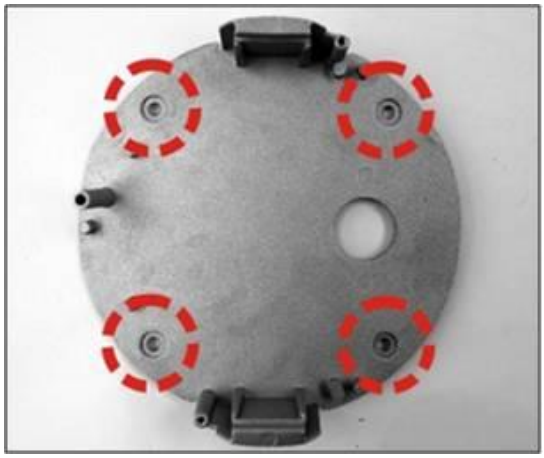


Figure 14: Base Plate Used as a Template to Mark Drilling Locations

     b) In the marked locations, drill each hole using a drill-bit of a slightly smaller diameter than the supplied screw anchors (molly-plug anchor). You want to achieve a snug insertion so that the plug expansion holds firm after the screws are screwed in.
     c) Fully insert the supplied anchors into drilled holes. You may need to tap them flush with the wall using a finishing hammer.
   - For installing on a 4S recessed electrical box:
     a) Have a qualified installer (check your local electrical codes) rough-in the 4S recessed electrical box and run the wires and power (if not PoE) through the wall/conduits to the box location.
     b) Ensure that the box is sufficiently sturdy (attach to the wall stud, ceiling joist, or reinforced surface as needed) to securely hold the weight of the camera.

- For bracket, pole and pendant installations:

  a) Thread the power and Ethernet cables and any other wires (such as a relay output, alarm input, audio in, or audio out) through the wire entry.

  b) If you are not wiring from within the wall, you can run the wires through the cable entry hole on the side of the dome.

  c) If necessary, you may need to unscrew the disk from the cable entry hole and screw it into the alternate unused conduit cable entry hole in order to seal it.

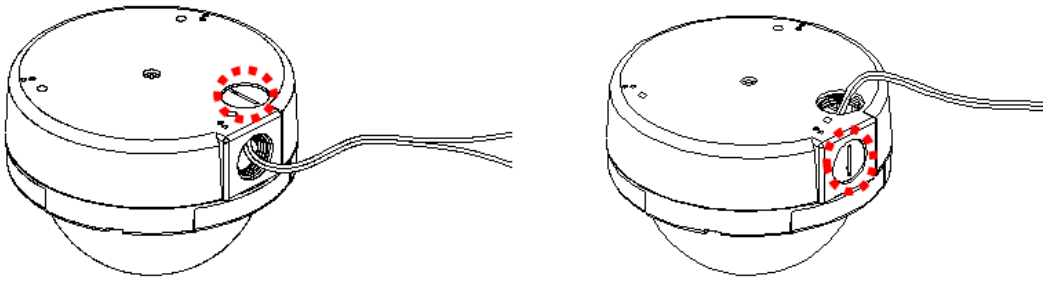


Figure 15: Top and Side Cable Entry Openings to Dome

Tip:
Even if you are not using alarm inputs and audio input/output at the time of installation, you may want to consider pre-wiring these connections for future use.

Note:
The power cable is not required if using PoE.

3. Thread the wires through the base plate and screw it to the predrilled wall, ceiling, CM Series Mini-Dome Recessed Mount, CM Series Mini Mini-Dome Corner Mount, or 4S electrical box. Check that the installation is not flimsy, will not wobble, and is flush with the mounting surface.

Tip:
Use shims for shoring up mounts on uneven surfaces.

4. Snap the camera module back on the base plate with the wiring threaded through the gap at the module base and then screw in the module-fastening screw.

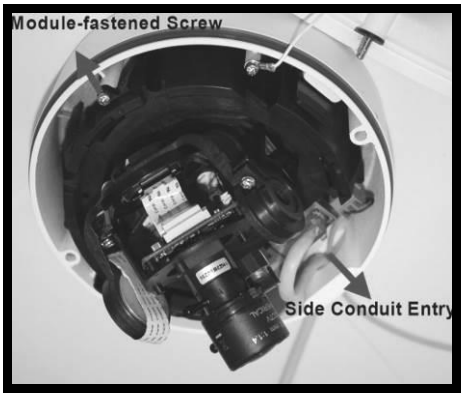


Figure 16: Replacing Camera Module onto Base Plate

5. Plug the Cat 5 cable into the camera Ethernet port and, if needed, plug the power terminal block into the power terminals.

6. If applicable, wire the Alarm In, Alarm Out, Audio In, and Audio-Out terminal blocks to external devices. See Figure 6: CM-3211/4221 Camera Input/Output Connections.
7. If needed, connect the other end of the Cat 5 cable to the network and turn on the power from the power supply.

> **Note:**
> Do not reassemble the camera's inner cover and Mini-Dome cover until after hardware configurations and lens adjustments are made.

6 Using the DNA Utility to Search and Access the Camera

6.1 Introduction

The DVTEL Network Assistant (DNA) is a user-friendly utility that is designed to easily discover and configure DVTEL edge devices on a network.

The DNA tool has a simple user interface and does not require any installation. The software is provided as a single, standalone executable. It runs on any PC.

DNA provides a central location for listing all the DVTEL CM, CF and CP camera models accessible over the network. Once listed, each camera can be right-clicked to access and change the network settings.

If the network settings are changed for some reason, a new search will relist the units. The units may then be configured via the web interface.

If DVTEL Latitude is being used, configure the unit with a static IP address rather than with DHCP. This ensures that the IP address will not automatically change in the future and interfere with configurations and communication.

The camera must be made accessible for the network's addressing.

Note:
DNA is an enhanced software alternative to Device Search. Either of these programs may be used.

To install DVTEL Web Player (DCViewer) software online:

Upon initial connection to the camera, a prompt to install the DVTEL Web Player (DCViewer) appears. If the web browser does not allow DVTEL Web Player to install, check the Internet security settings or ActiveX controls and plug-in settings to continue the process. See Appendix A.3 Internet Security Settings.

Caution:
Users who have previously installed the DVTEL Web Player (DCViewer) on the PC should delete the existing DCViewer from the PC before accessing the camera. For information on how to uninstall and clear Temporary Internet Files, see Appendix A5: Deleting the Existing DCViewer.

6.2 Quick Start

To start using the DNA application:

1. Install and run the DNA application on a computer connected to the network. The software is an `.exe` file supplied in a zip file together with an Online Help file (`.chm`).
2. Extract both files from the zip file, and place them together in a new directory. Both files should have the same name, but different extensions (`.exe` and `.chm`).
3. Upon launching the tool, DNA automatically discovers all devices on the network. The initial launch creates a default `.ini` file (`dna.ini`).
4. In the event that there are devices that are not authenticated, click **Login** and enter login credentials for the devices.

5. If there are devices located on a separate VLAN, the devices must be added manually. Click **Add Device Manually** from the Operational Toolbar and add the devices.

6.3 Main Screen

The DNA main screen contains four sections, as seen in the following figure:

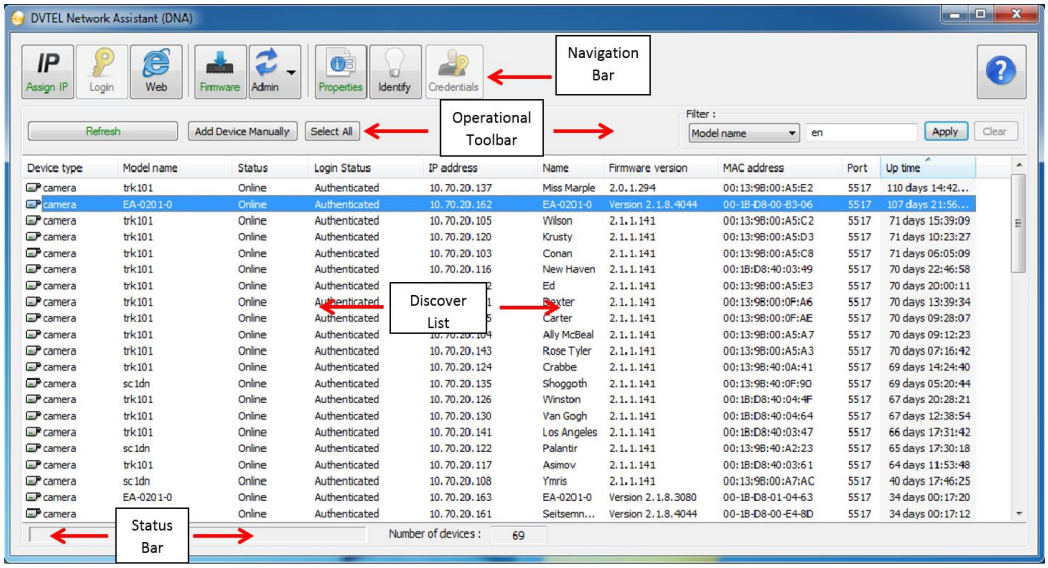


Figure 17: DNA Main Screen

6.4 Navigation Bar

The callouts on the screen are explained below:

1. Navigation Bar: Located at the top of the screen. Includes tabs and dropdown menus to perform actions.
2. Operational Toolbar: Located below the Navigation Bar. Used to refresh discovered units, filter connected devices for easy operation, and to add a device manually.
3. Discover List: Occupies the center of the screen. Displays a list of discovered devices with partial device information.
4. Status Bar: Located at the bottom of the screen. Displays current device status, including scanning time, status, and the number of discovered units.

The Navigation Bar contains tabs for all the actions needed to configure and manage attached devices. If no devices have been discovered, all the tabs are gray (disabled).

After a device has been discovered, the tabs for functions which it supports are enabled and colored, as seen in the following Figure:

To define the device on which to perform an action, the user must select the device from the Discover List. The user can select more than one device, in which case the action will be done on all selected devices.

6.5 Context Menu

All functions on the Navigation Bar are also accessible from the context menu, which is available when right-clicking on a device within the Discover List, as seen in the following figure:

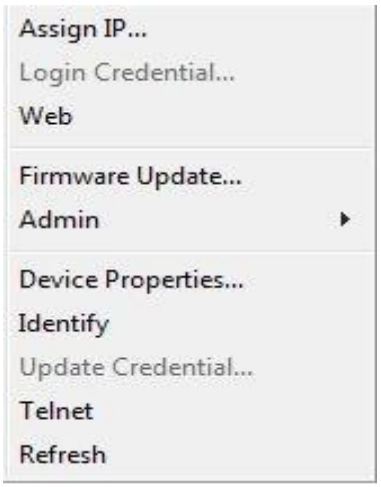


Figure 18: Context Menu

Assign IP Tab

The **Assign IP** tab or context menu option is used to automatically assign the IP address of the selected device(s). This function can be used for automatic batch network configuration.

The **Assign IP** tab or context menu option is used to automatically assign the IP address of the selected device(s). This function can be used for automatic batch network configuration. The **Assign IP** tab or context menu option is grayed if a device has not been selected.

Selecting this tab or option opens the **Assign IP** window, which displays a list of devices which need to be updated, as shown in the illustration below. The **Assign IP** window is divided into two areas See section 6.6 for more details.

6.6 Configuring Communication Settings on the Quasar Camera

1. Connect the camera to the network on the same VLAN/LAN as the workstation.
2. If the network supports the default, open DNA utility by running dna.exe which can be found in the DNA Utility folder in the supplied CD.

Note:
DNA is an alternative software to Device Search. Either of these programs may be used.

3. In the DNA application, click the **DNA** button.
4. If the Windows Firewall is enabled, a security alert window pops up.

5. To continue, click **Allow Access**. Latitude users should consult the Latitude Installation Instructions on disabling the Windows Firewall.

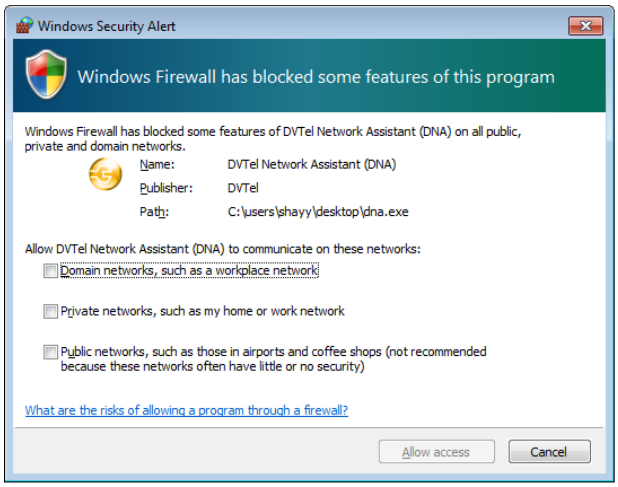

Windows Security Alert
Windows Firewall has blocked some features of this program
Windows Firewall has blocked some features of DVTel Network Assistant (DNA) on all public, private and domain networks.
Name: DVTel Network Assistant (DNA)
Publisher: DVTel
Path: C:\users\shayy\desktop\dna.exe
Allow DVTel Network Assistant (DNA) to communicate on these networks:
Domain networks, such as a workplace network
Private networks, such as my home or work network
Public networks, such as those in airports and coffee shops (not recommended because these networks often have little or no security)
What are the risks of allowing a program through a firewall?
Allow access
Cancel

Figure 19: Windows Firewall Screen

6. Click **Assign IP**. All the discovered IP devices will be listed in the page, as shown in the figure below. The camera's default IP Address is automatically supplied by the DHCP server.

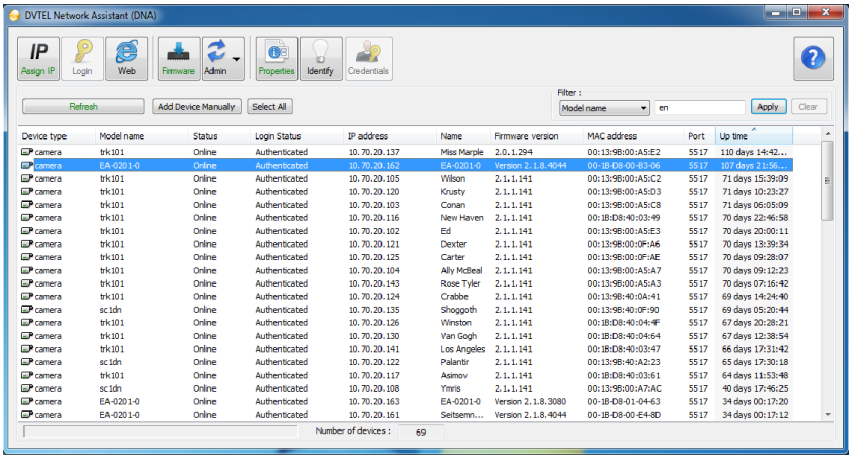


Figure 20: Discovered IP Devices

7. Right-click the camera whose network property is to be changed. From the menu that opens, select **Network Setup**. The **Network Setup** dialog is displayed.

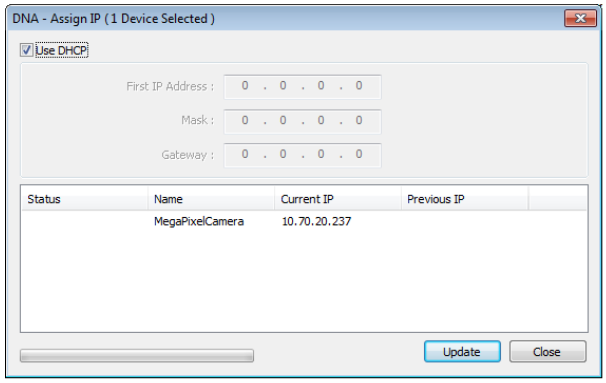


Figure 21: DNA Assign IP – Use DHCP Dialog Box

Tip:
Record the camera's MAC address for future reference.

8. To access DNA, do one of the following:
   a) For DHCP (not supported by Latitude):
      i. Select *Use DHCP*. Do not use for Latitude.
      ii. Click **Update** and wait for status.
   b) For Static IP (recommended for Latitude users):

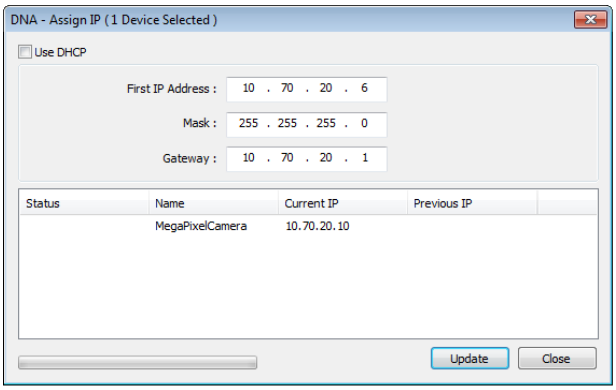


Figure 22: DNA Assign IP – Static IP Dialog Box

      i. Do not select the *Use DHCP* checkbox. This is recommended for security purposes and for and Latitude users. In the IP Address, Gateway, and Netmask, enter the respective LAN/VLAN (optional DNS) values.
      ii. Click **Update** and wait for *OK* status to be displayed.
9. Right-click and select **Browse** to directly access the camera via a web browser. The default web browser opens and requests access to the camera IP address.
10. When the web browser contacts the camera IP, do the following:
    a) Login using the default user name *Admin* and password *1234*.

Note:
ID and password are case-sensitive.

Note:
It is strongly advised that administrator's password be altered for security reasons.

b) If the Information Bar (just below the URL bar) prompts for permission to install the ActiveX Control for displaying video in the browser (see the figure below), right-click on the Information Bar. Select **Install ActiveX Control** to allow the installation.

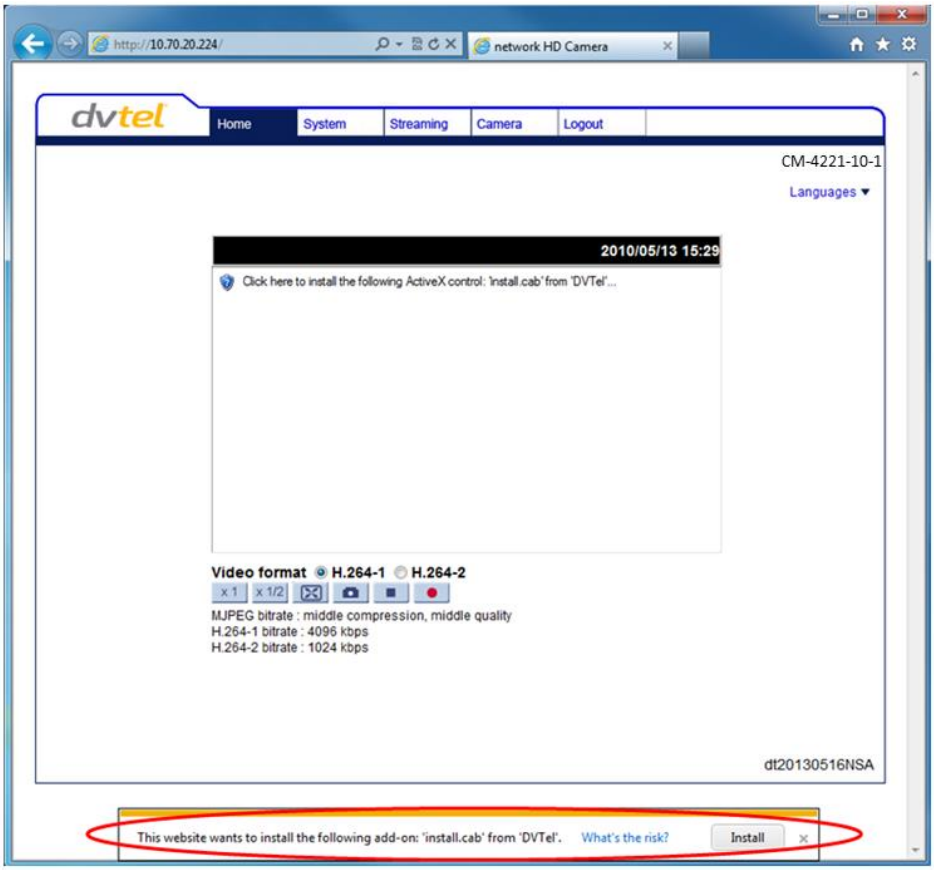


Figure 23: Installing the ActiveX Control

If a security warning window prompt appears, click **Install**.

Internet Explorer - Security Warning
Do you want to install this software?
Name: DVTel Web Player
Publisher: DVTel
More options
Install
Don't Install
While files from the Internet can be useful, this file type can potentially harm your computer. Only install software from publishers you trust. What's the risk?

Figure 24: Security Window

11. If the wizard appears for installing the component application DCViewer, follow the instructions to complete the installation.

> **Note:**
> If the password is changed and DVTEL Latitude AdminCenter Discovery feature is in use, deselect all other proprietary types. Select **DVTEL HD Series** so that the new password can be configured in the Discovery tab settings.

Additionally, users can change the camera's network property (either DHCP or Static IP) directly in the device finding list. Refer to the following section for changing the camera's network property.

6.7 Adjusting and Framing-Up the Camera View

After the camera is connected to the network and running, it is necessary to frame-up the scene and adjust the camera settings to optimize the picture for the individual scenes. If Latitude is being used, consider scheduling different settings for changing ambient conditions throughout the day, week, month or seasons.

To adjust and frame-up the camera view:

1. In the DNA application, click **DNA**.
2. In the results, click to select the camera.
3. Right-click to open the shortcut menu, and select **Browse**, or enter the camera's IP address in your Internet browser's URL address bar.
4. When the Internet browser connects to the camera and prompts for login, do the following:
    a) Log in using the default user name *Admin* and password *1234*. If the password has previously been changed, use the new password.
    b) Allow the ActiveX to download and choose to install the DVTEL Web Player (DCViewer).
5. On the camera, loosen the screw on the tensioning collar of the camera tilt axis.

6. On the camera, adjust the rotation, pan and tilt angles as required for the desired view of the scene. When finished, retighten the tilt-arm tension screw.

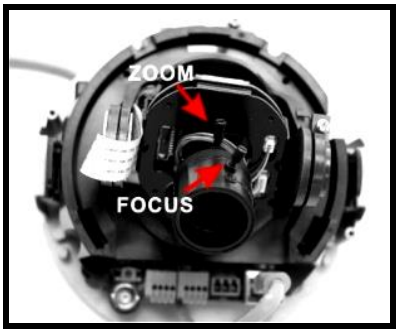
Figure 25: CM-3211/4221 Camera – Pan, Rotate and Tilt Angles

Caution:
To prevent camera damage, do not over extend the tilt range beyond -10° to 90°.

Tip:
To view greater image detail for more accurate high-definition focusing, on the Web Base Viewer home page, click **Full Screen** and check the focus.

Note:
Best focusing results can be achieved when the lens iris is fully open (such as at night in low light). This prevents loss of sharpness if light levels are reduced at night.

7. To achieve optimum focus results during daytime, go to the Camera > Exposure screen in the Web Base Viewer and, from the Exposure Setting menu, select Auto-shutter mode. Save changes and complete the focusing steps. When finished, restore your exposure settings as needed.
8. Adjust the zoom ring and focus ring for your scene.



9. Replace the camera's inner cover.
10. Replace the Mini-Dome cover and tighten the screw.

7 Configuration and Operation

The Quasar CM series camera is provided with a browser-based configuration interface for video playback and recording. In this chapter, information about main page introduction, system related settings and camera settings are described in detail.

Additionally, if DVTEL's Latitude VMS is used, many of the configurations and features of DVTEL's VMS provide configuration and automation of the camera.

This section includes the following information:

- Browser-Based Viewer Introduction
- Home Page
- System-Related Settings
- Video and Audio Streaming Settings
- Camera-Related Settings
- Logout

7.1 Browser-Based Viewer Introduction

The figure below shows the Quasar camera's browser-based user interface.

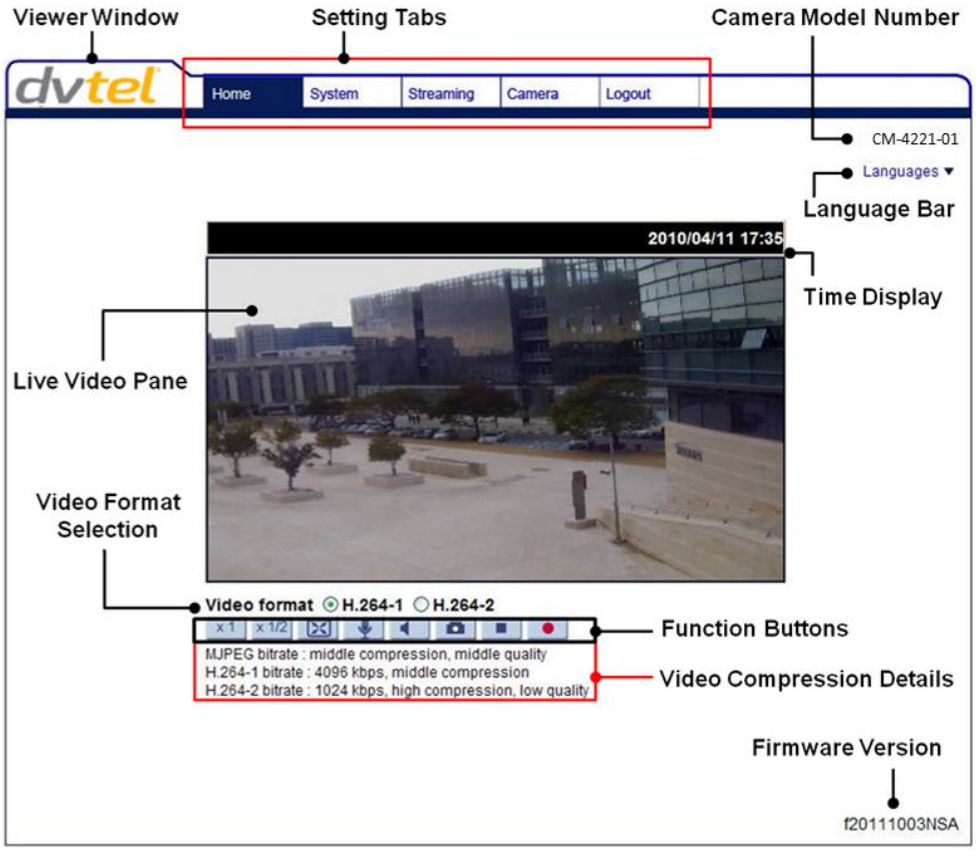


Figure 26: Quasar Browser-Based User Interface

- At the top of the Viewer Window is the Navigation Bar, which contains five main tabs: Home, System, Streaming, Camera, and Logout.
  - Home Page
    Users can monitor live video of the targeted area, adjust the display size including use of the digital zoom feature, activate or de-activate the speaker (audio function), take snapshots of the view area, stop/start video streaming, and record video in a designated storage place. Further details are discussed in Home Page.
  - System Settings
    The administrator can set host name, system time, root password, network related settings, etc. Further details are discussed in System-Related Settings.
  - Streaming Settings
    The administrator can modify video resolution and picture rotation and select audio compression mode on this page. Further details are discussed in Video and Audio Streaming Settings.
  - Camera Settings
    The administrator can adjust many of the camera settings on this page, such as Exposure, White Balance, Picture, Backlight, Digital Zoom, IR Function, WDR Function, Noise Reduction, and TV System. Further details are discussed in Camera-Related Settings.

    Note:
    The IR Function is only available on the CM-3211/4221-10-I and CM-3211/4221-11-I cameras.
  - Logout
    Click on the tab to re-login the camera with another username and password. See Logout.
  - Callouts
    - In the top right-hand corner of the Viewer window, the Camera Model Number is displayed.
    - Below the camera model number is the Language Bar. Supported languages include English, German, French, Italian, Simplified Chinese, Traditional Chinese, Russian, and Korean.
    - In the center of the Viewer window is the Live View pane, which displays the image that the camera is monitoring.
    - On the right side of the black bar at the top of the Live View pane is the Time Display.
    - Under the Live View pane is the Video Format selection, enabling H.264-1 or H.264-2 to be selected.
    - Below the Video Format selection are the Function buttons, which are discussed in the following section.
    - Under the Function buttons are the Video Compression details, including bit rate, compression, and quality.
    - In the bottom right-hand corner of the Viewer window, the Firmware Version of the camera is displayed.

7.2 Home Page

The CM-3211/4221 series includes two types of cameras. One type features a variable focus (varifocal) lens. The second type features a motorized lens. Each type has its own specific home page.

7.2.1 CM-3211/4221-00/01 Varifocal Camera Home Page

All models in the CM-3211/4221-xx series include the following function buttons located on the **Home** page shown below.

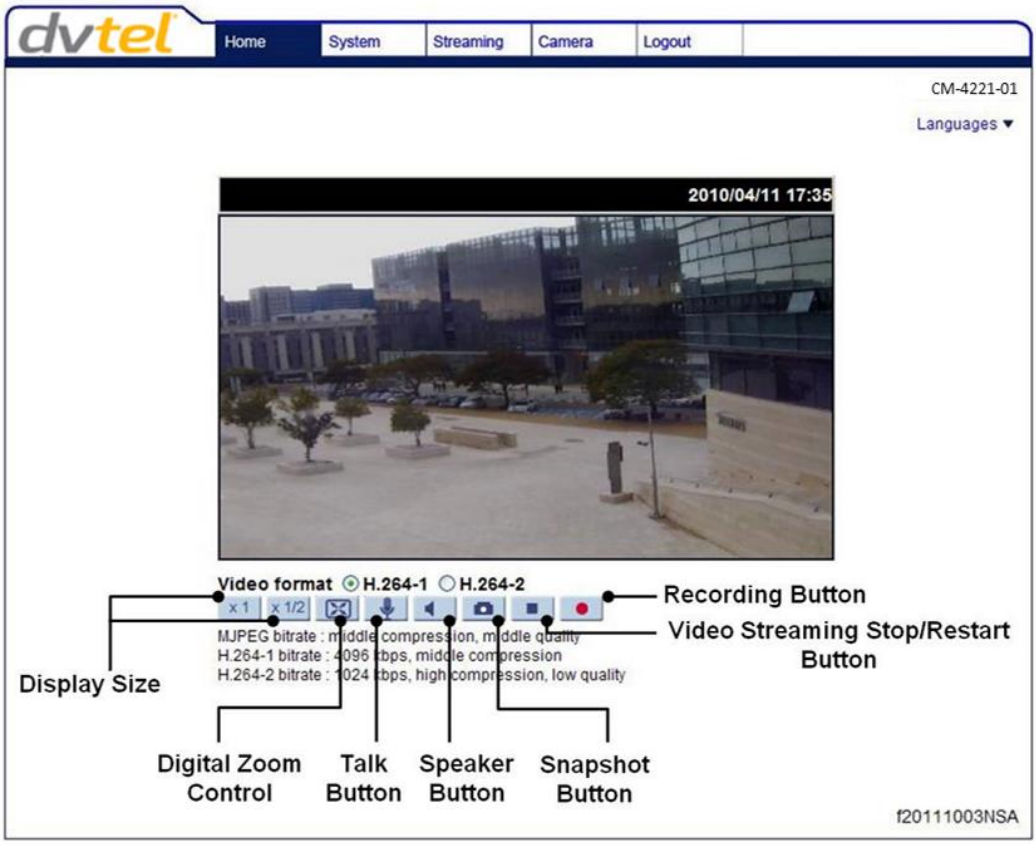


Figure 27: Home Page Function Buttons – for Varifocal Cameras

- **Display Size Adjustment (x1/x½)**
  The image display size can be adjusted to full-size or half-size.

- **Full Screen Mode** (with Digital Zoom Control)
  Click this button to view the monitored image in full screen mode. Use the mouse to control zoom effects in Full Screen mode: scroll the mouse wheel (for zoom in/out), and drag the mouse into any direction. Double-click on the screen to exit Full Screen mode and return to the **Home** page.

- **Talk**
  The **Talk** button allows the local site to talk to the remote site. Click the button to switch it on/off. This function is available only to a user who has been granted this privilege by the Administrator. Refer to User in the Security section for further details.

- **Speaker**
  Press the **Speaker** button to mute/activate the audio. This function is available only to a user who has been granted this privilege by the Administrator. Refer to User in the Security section for further details.

- **Snapshot**
  Press this button to automatically save the JPEG snapshots in the specified location. The default location to save snapshots is: C:\.To change the storage location, refer to File Location.
- **Video Streaming Stop/Restart**
  Press the **Stop** button to disable video streaming and to display the live video as black. Press **Restart** to show the live video again.
- **Recording**
  Pressing the **Recording** button stores recordings from the Live View in the location specified on the local hard drive, which can be configured in the **File Location** screen. The default storage location for the web recording is: C:/. Refer to File Location for details.

7.2.2 CM-3211/4221-10/10-I/11/11-I Motorized Camera Home Page

The CM-3211/4221-10, CM-3211/4221-10-I, CM-3211/4221-11, and CM-3211/4221-11-I cameras feature a motorized lens. The **Home** page also includes the following function buttons in addition to those shown for the CM-3211/4221-00/01.

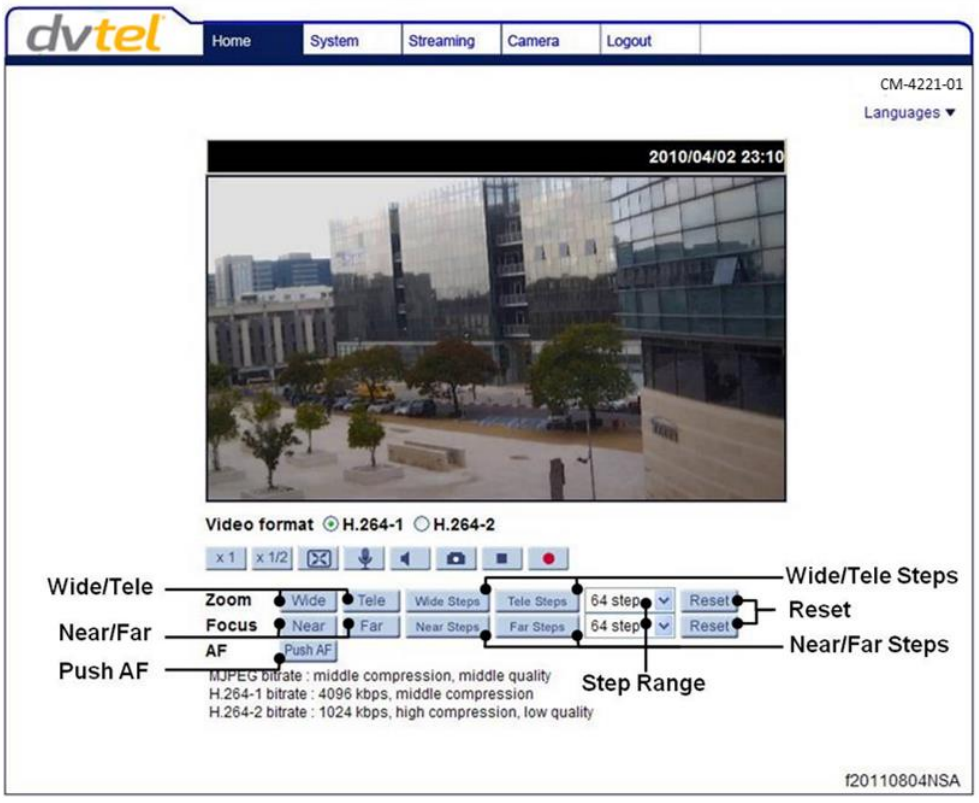


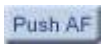
Figure 28: Home Page Function Buttons – for Cameras with Motorized Lens

Wide/Tele

Press the **Tele** or **Wide** button to implement continuous zoom adjustment.

Near/Far

Press the **Near** or **Far** button to implement continuous focus adjustment.

Push AF 

Press the **Push AF** button once to adjust zoom or focus.

Wide Step/Tele Step

Press the **Wide Step** or **Tele Step** button to alternate the zoom between wide and telephoto views within a user-defined range of steps, which can be selected from the drop-down menu shown below.

Near Step/Far Step

Press the **Near Step** or **Far Step** button to alternate the focus between near and far views within a user-defined range, which can be selected from the drop-down menu.

Reset

Press the **Reset** button to calibrate the camera lens at full wide end and infinity focus simultaneously.

Step Range

Select from a user-defined range of steps, which can be selected from the drop-down menu below.

Figure 29: Home Page – Step Range Drop-Down Menu

7.3 System-Related Settings

The figure below shows all categories under the **System** tab. Each category in the sidebar is explained in the following sections.

> **Note:**
> The **System** configuration screen is accessible only by the Administrator.

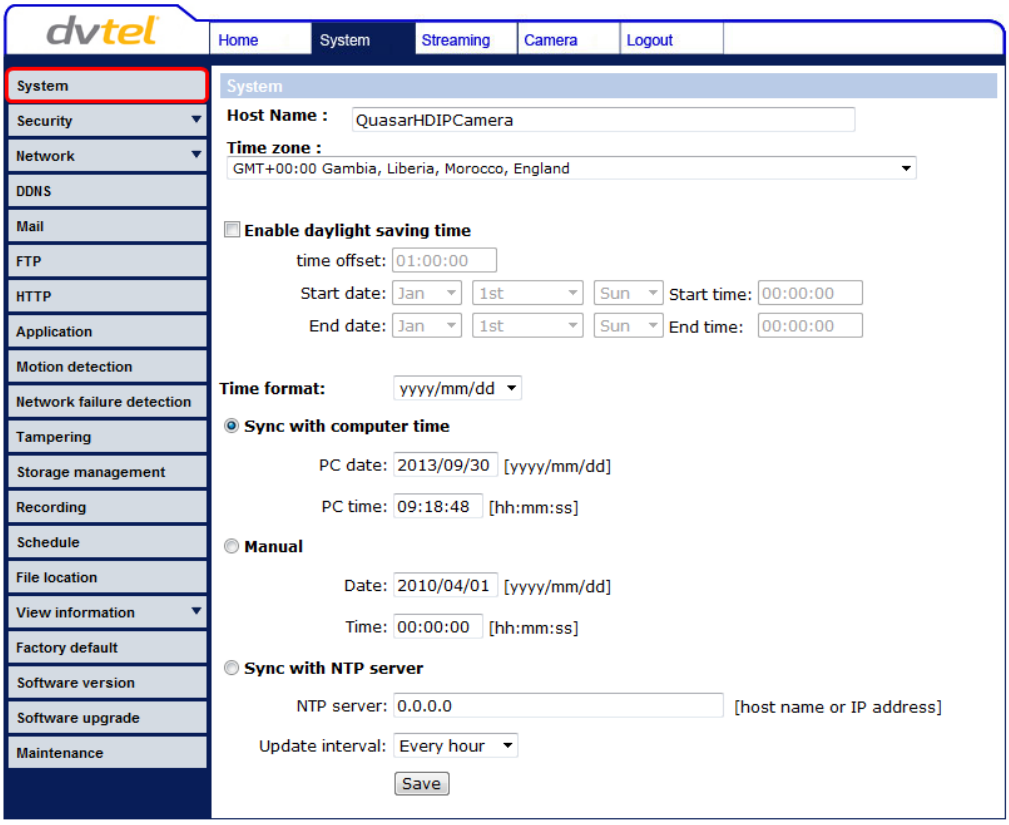


Figure 30: System Screen

Related Links

- System
- Security
- Network
- DDNS
- Mail
- FTP
- HTTP
- Application
- Motion Detection
- Network Failure Detection
- Tampering Alarm
- Storage Management
- Recording
- Schedule
- File Location
- View Information
- Factory Default
- Software Version
- Software Upgrade
- Maintenance

7.3.1 System

Click the **System** tab in the sidebar. The **System** page is displayed in Figure 30: System Screen. It includes the following details:

Host Name

The host name is for camera identification. If the alarm function is enabled and is set to send an alarm message by Mail/FTP, the host name entered here is displayed in the alarm message. See Application.

Time Zone

Select the time zone from the drop-down menu.

Enable Daylight Saving Time

To enable DST, check the box and then specify time offset and DST duration. The format for time offset is [hh:mm:ss]. For example, if the amount of time offset is one hour, enter 01:00:00 in the field.

Time format

Enables a choice of formats: either year, month and day (yyyy/mm/dd) or day, month and year (dd/mm/yyyy).

Sync with Computer Time

Select this button to synchronize video date and time display with the PC.

Manual

The Administrator can set video date, time and day manually. Entry format should be identical with that displayed to the right of the text box.

Sync with NTP Server

Network Time Protocol (NTP) is an alternate way to synchronize the camera's clock with an NTP server. Specify the server to synchronize in the text box. Then select an update interval from the drop-down menu. For further information about NTP, visit www.ntp.org.

7.3.2 Security

Clicking the category **Security** in the System sidebar opens a drop-down menu with the tabs **User**, **HTTPS**, **IP Filter** and **IEE 802.1X**.

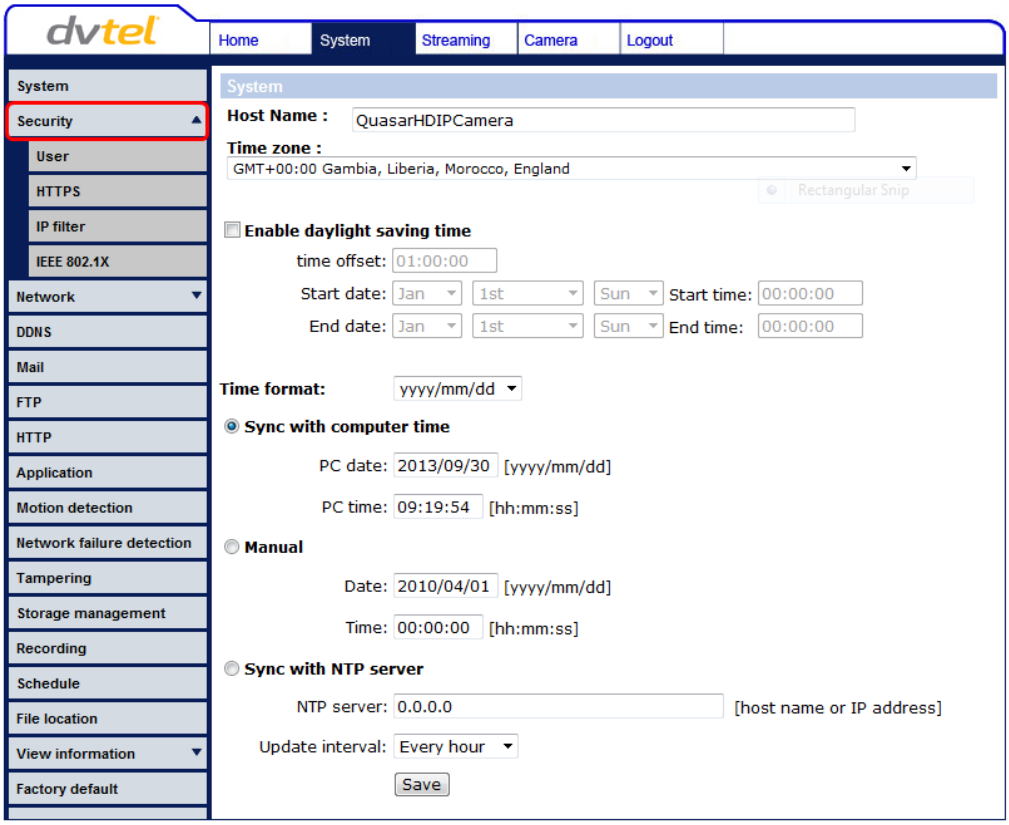


Figure 31: System Configuration – Security

Related Links

- User
- HTTPS
- IP Filter
- IEEE 802.1X

7.3.2.1 User

Click the **User** tab in the **Security** category on the sidebar to display user credentials.

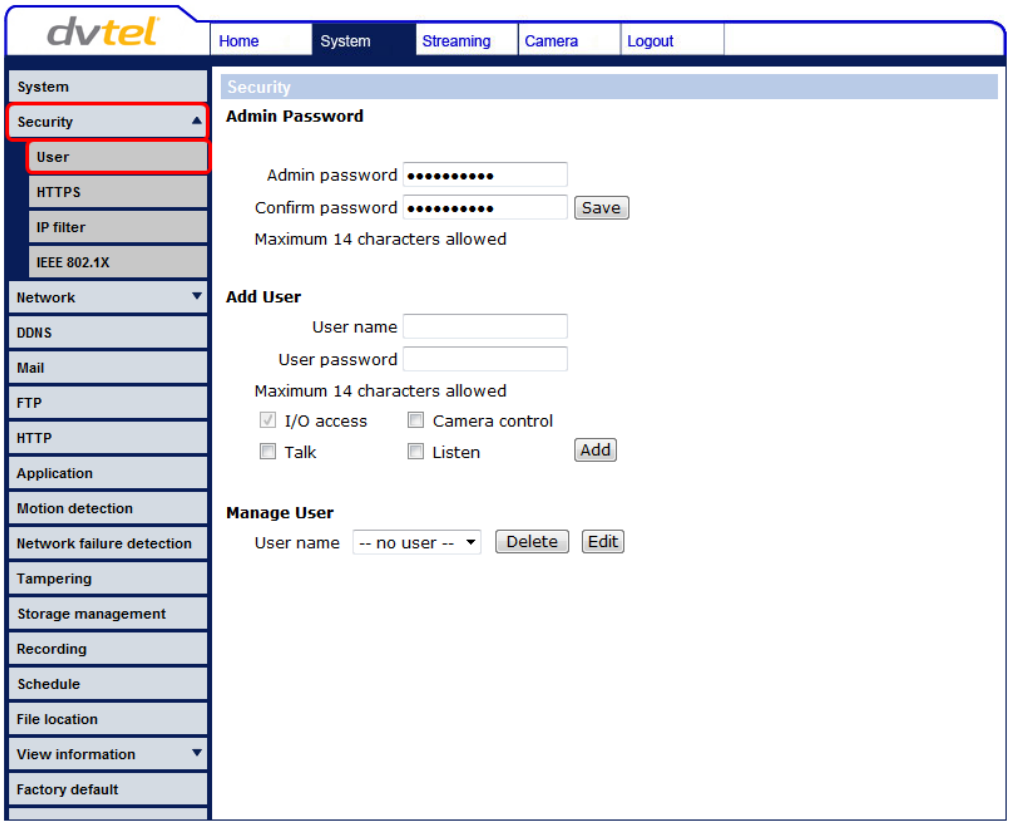


Figure 32: Security Screen

Admin Password

Change the administrator's password by entering the new password in both text boxes. The input characters/numbers are displayed as dots for security purposes. After clicking **Save**, the web browser asks the Administrator for the new password (maximum 14 digits).

Note:
The following characters are valid: A-Z, a-z, 0-9,!#$%&'-.@^_~.

Add user

The user name and passwords are limited to 14 characters. There is a maximum of 20 user accounts.

To add a new user:

1. Type the new user name and password in the respective fields.
2. Select the appropriate check boxes to give the user Camera Control, Talk and Listen permissions.
   - *I/O access* – Basic functions that enable you to view video when accessing to the camera.
   - *Camera control* – Allows you to change camera parameters on the **Camera** tab.
   - *Talk/Listen* – *Talk* and *Listen* functions allow the user at the local site to communicate with the administrator at the remote site.
3. Click **Add**.

Manage User

- To delete a user, pull down the user list and select the user name to delete. Click **Delete** to remove it.
- To edit a user, pull the user list down and select a user name. Click **Edit** to edit the user's password and privileges.

Figure 33: Editing Password and Privileges

Note:
You must enter the user password and also select the authorized function(s). When finished, click **Save** to modify the account authority.

Figure 34: Modifying Account Authority

7.3.2.2 HTTPS

To use HTTPS on the camera, an HTTPS certificate must be installed. The HTTPS certificate can be obtained either by creating and sending a certificate request to a Certificate Authority (CA) or by creating a self-signed HTTPS certificate as described below.

Note:
The self-signed certificate does not provide the same level of security as a CA-issued certificate.

HTTPS allows secure connections between the camera and web browser using Secure Socket Layer (SSL) or Transport Layer Security (TLS) to protect camera settings and username/password info. A self-signed certificate or a CA-signed certificate is required to implement HTTPS. Under the **Security** category, click the **HTTPS** tab in the sidebar to display the following screen.

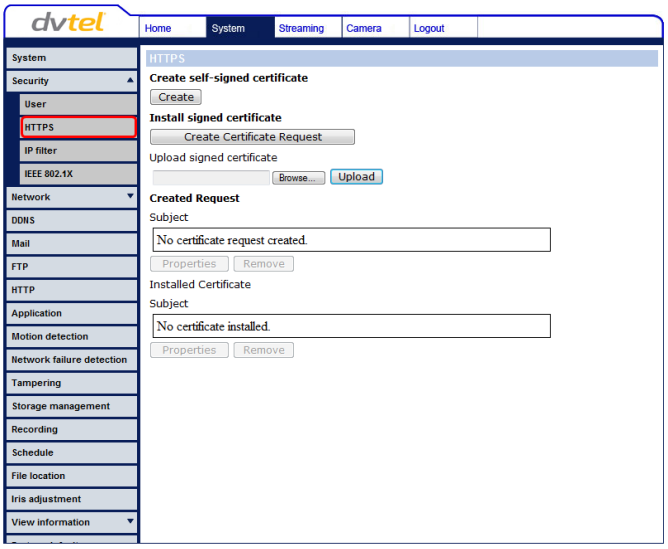


Figure 35: HTTPS Screen

To create a self-signed certificate:

Before a CA-issued certificate is obtained, users can first create and install a self-signed certificate.

1. On the **HTTPS** page, click **Create** under *Create self-signed certificate.*
2. Provide the requested information to install a self-signed certificate for the camera. Refer to *Provide the Certificate Information* in this section for details.

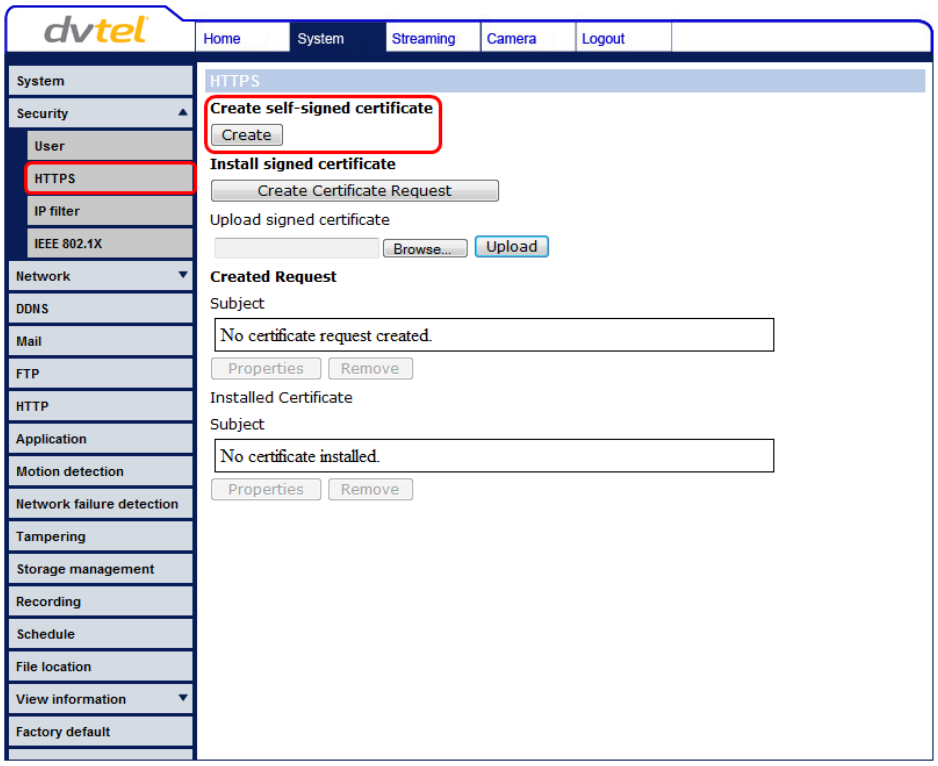


Figure 36: HTTPS Screen – Create Self-Signed Certificate

To create a certificate request:

1. Click **Create Certificate Request** to create and submit a certificate request in order to obtain a signed certificate from a CA**.**
2. Provide the requested information in the *Created Request* field. Refer to *Provide the Certificate Information* in this section for details.
3. When the request is complete, the subject of the *Created Request* is shown in the field. Click **Properties** below the *Subject* field, copy the PEM-formatted request and send it to your CA.

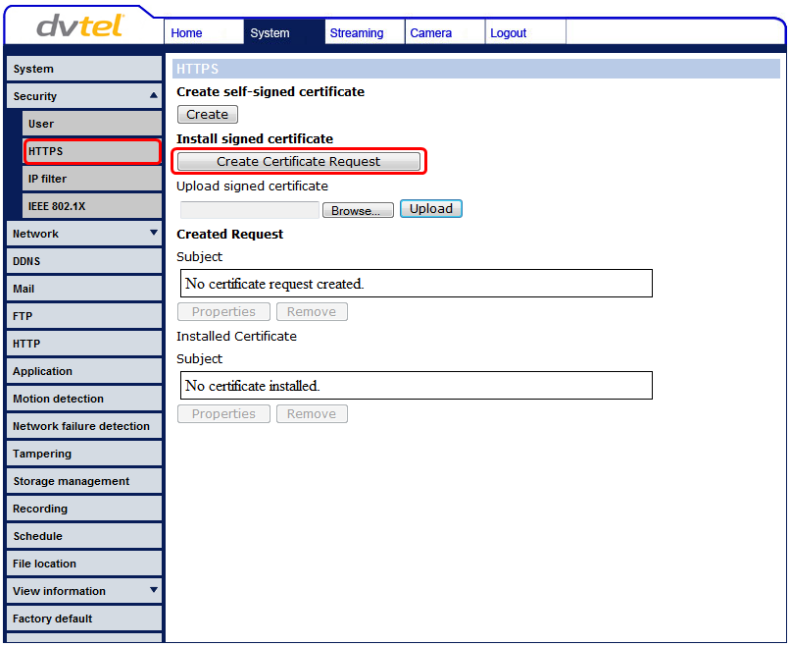


Figure 37: HTTPS Screen – Install Signed Certificate

4. When the signed certificate is returned from the CA, install it by uploading the signed certificate as seen in Figure 38.

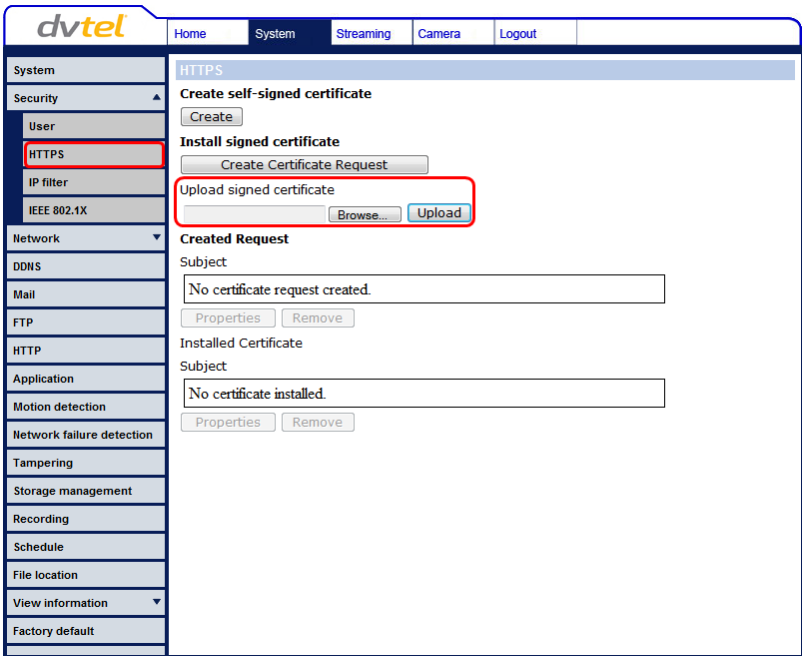


Figure 38: HTTPS Screen – Upload Signed Certificate

To provide the certificate information:

To create a self-signed HTTPS certificate or a Certificate Request to CA, enter the information in the **Create a Self-signed Certificate** screen. A definition of each of the requested fields follows.

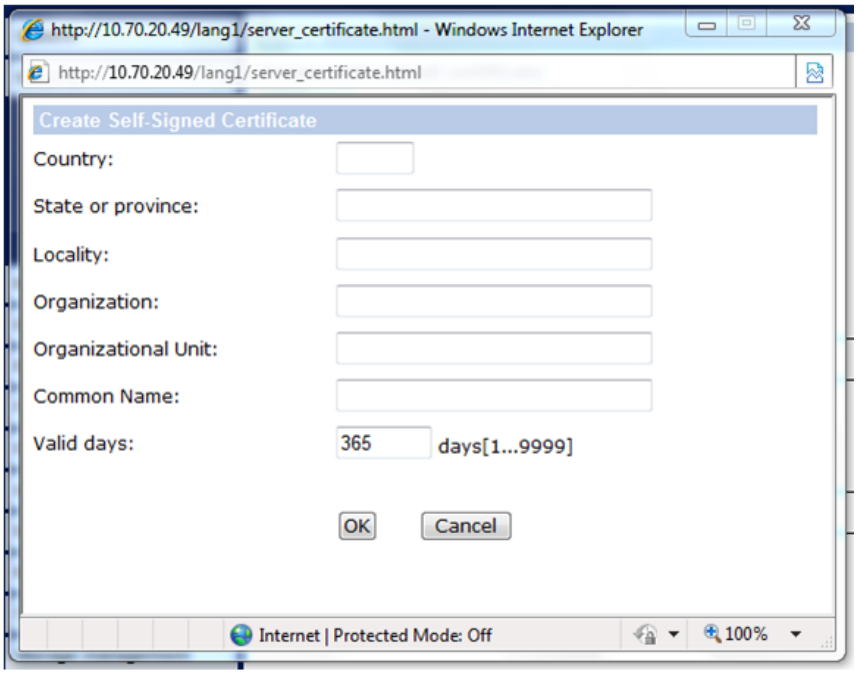


Figure 39: Example of Self-Signed Certificate

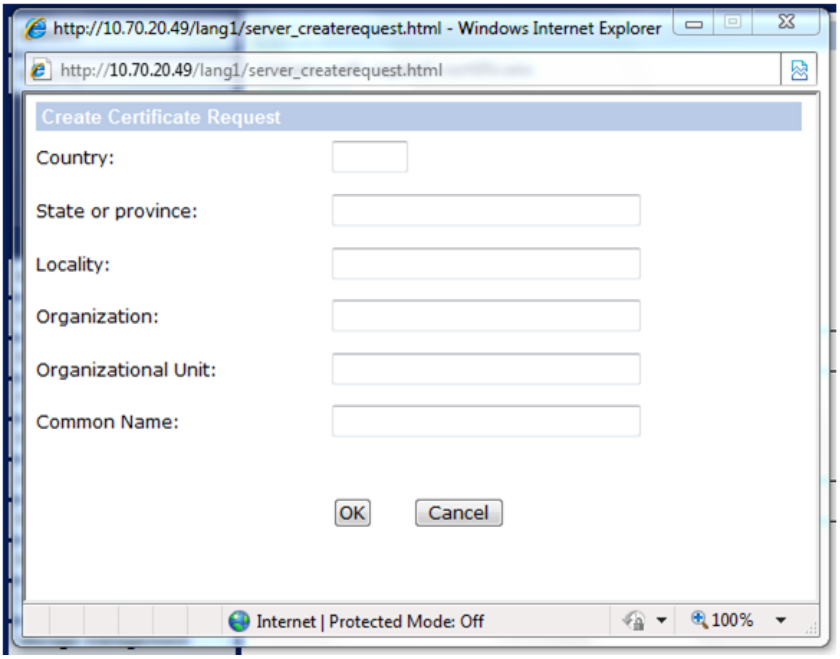


Figure 40: Self-Signed Certificate – Details

5. Provide the requested information to install a self-signed certificate for the camera.
   - *Country* – Enter a two-letter combination code to indicate the specific country in which the certificate will be used. For instance, type "US" to indicate United States.
   - *State or province* – Enter the local administrative region.
   - *Locality* – Enter other geographical information.
   - *Organization* – Enter the name of the organization to which the entity identified in *Common Name* belongs.
   - *Organizational Unit* – Enter the name of the organizational unit to which the entity identified in the *Common Name* field belongs.
   - *Common Name* – Indicate the name of the person or other entity that the certificate identifies (often used to identify the website).
   - *Valid days* (self-signed certificate only) – Enter the period in days (1 ~ 9999) to indicate the valid period of certificate.
6. Click **OK** to save the certificate information after completion.

Note:
The self-signed certificate does not provide the same high level of security as a Certificate Authorized (CA)-issued certificate.

7.3.2.3 IP Filter

The IP filter restricts access to the camera by denying/allowing specific IP addresses. Click the **IP filter** tab under the category **Security** in the sidebar to display the following page.

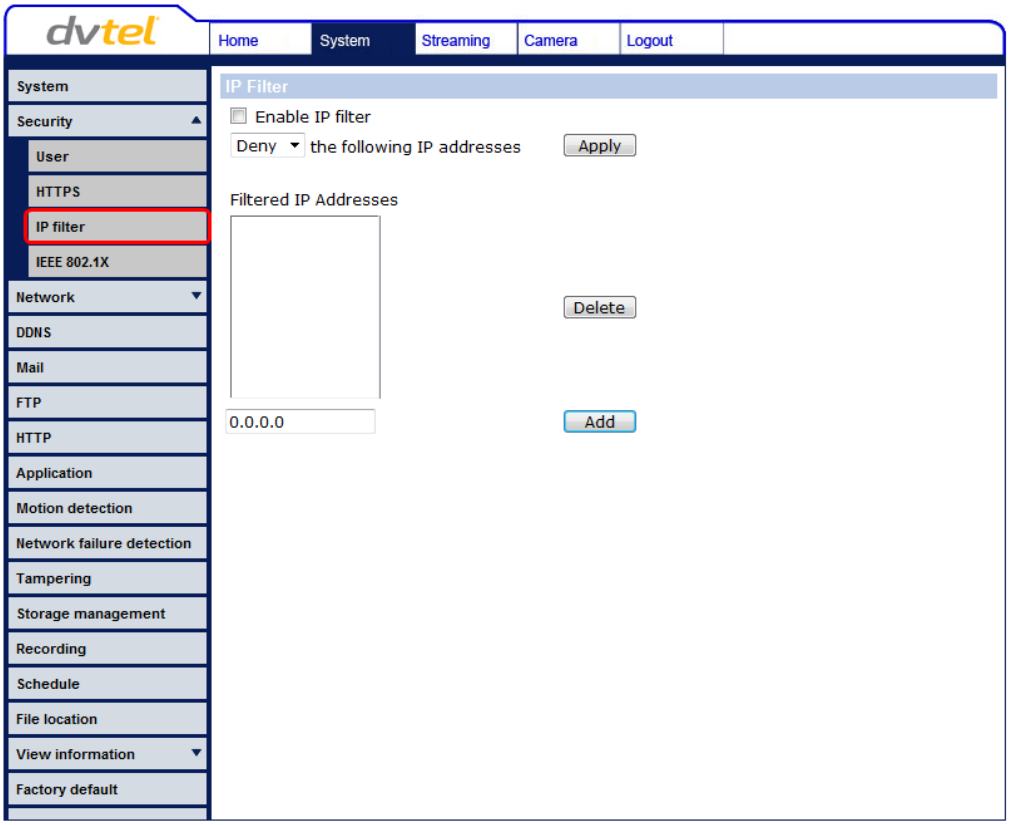


Figure 41: IP Filter Screen

Enable IP Filter

1. Check the box to enable the IP Filter function. Once enabled, the listed IP addresses (IPv4) are allowed/denied access to the camera.
2. Select *Allow* or *Deny* from the drop-down menu.
3. Click **Apply** to determine the IP Filter behavior.

Add/Delete IP Address

1. Enter the IP address in the *Filtered IP Addresses* text box.
2. Click **Add** to add a new filtered address. The *Filtered IP Addresses* box shows the currently configured IP addresses. Up to 256 IP address entries may be specified.
3. To remove an IP address from the list, select the IP address and then click **Delete**.

7.3.2.4 IEEE 802.1X

The camera is allowed to access a network protected by 802.1X/EAPOL (Extensible Authentication Protocol over LAN). Users must contact the network administrator to obtain certificates, user IDs, and passwords.

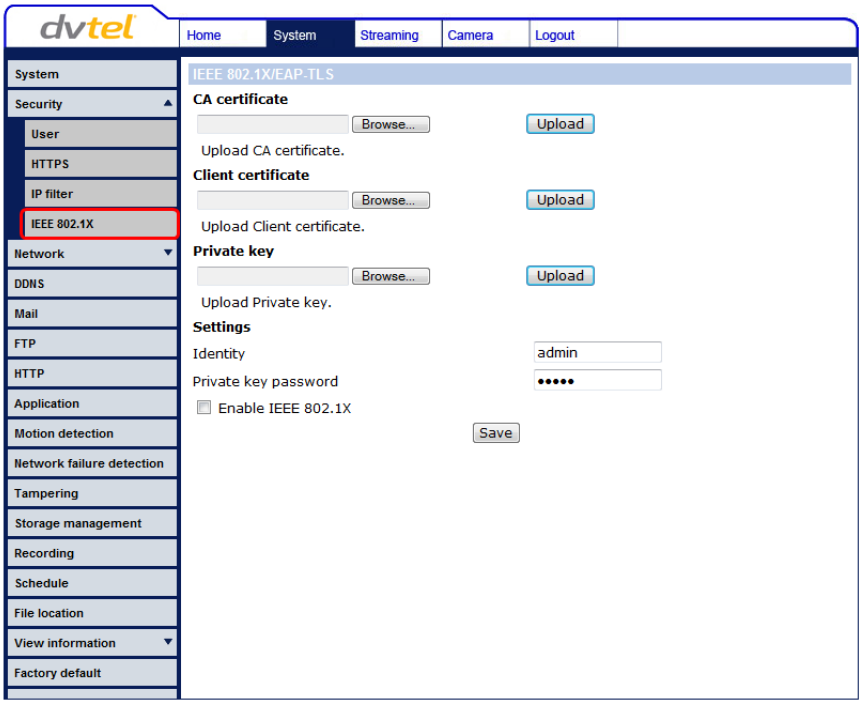


Figure 42: IEEE 802.1X/EAP-TLS Screen

CA Certificate

The CA certificate is created by the Certificate Authority for the purpose of validating itself. Upload the certificate to check the server's identity.

Client Certificate/Private Key

Upload the Client Certificate and Private Key to authenticate the camera.

Settings

- *Identity* – Enter the user identity associated with the certificate. Up to 16 characters can be used.
- *Private Key Password* – Enter the password associated with the user identity. Up to 16 characters can be used.

Enable IEEE 802.1X

Check the box to enable IEEE 802.1X. Click **Save** to save the IEEE 802.1X/EAPTLS setting.

7.3.3 Network

From the **System** screen, click the **Network** tab. A drop-down menu appears with tabs including **Basic**, **QoS**, **SNMP**, and **UPnP**.

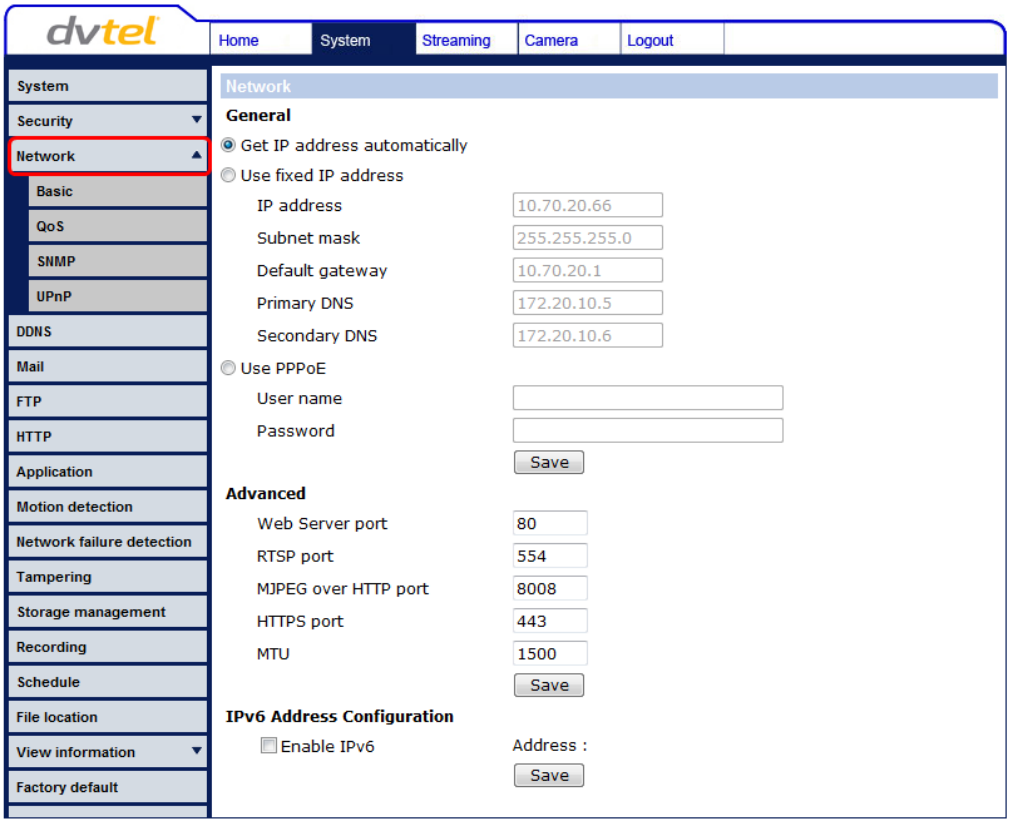


Figure 43: Network Screen

Related Links

- Basic
- QoS (Quality of Service)
- SNMP Settings
- UPnP

7.3.3.1 Basic

You can connect to the camera with either fixed or dynamic (DHCP) IP address. The camera also provides PPPoE (Point-to-Point Protocol over Ethernet) support for users who connect to the network via PPPoE.

The screen is divided into three sections: General, Advanced and IPv6 Configuration. See Figure 43: Network Screen.

1. **General**

Select one of the following options in the *General* area for configuring network settings:

- **Get IP address automatically (DHCP)**

If you select *Get IP address automatically*, you can use the DNA utility, which is provided in the supplied CD, to obtain the IP address. See Using the DNA Utility to Search and Access the Camera.

Note:
For future reference, record the camera's MAC address, which is found on the camera label.

- **Use fixed IP address**

The camera's default setting is *Use fixed IP address*. Refer to Using the DNA Utility to Search and Access the Camera for login with the default IP address. You may use DNA or enter the IP address in your Internet browser's URL address bar.

To set up a new static IP address:

1. Select the Use fixed IP address option.
2. Enter the following information:
   - *IP address* – The IP address is necessary for network identification.
   - *Subnet mask* – Used to determine if the destination is in the same subnet. The default value is 255.255.255.0.
   - *Default gateway* – Used to forward frames to destinations in a different subnet. An invalid gateway setting causes transmission to destinations in other subnets to fail.
   - *Primary DNS* – The primary domain name server that translates host names into IP addresses.
   - *Secondary DNS* – A secondary domain name server that backs up the primary DNS.
   - *Use PPPoE* – PPPoE users should enter their PPPoE user name and password into the respective fields.
3. Click **Save** to confirm the settings.

2. **Advanced**

Enter the following advanced parameters in the *Advanced* section of the screen:

- *Web Server port* – The default web server port is 80. Once the port is changed, the user must be notified the change for the connection to be successful. For instance, when the Administrator changes the HTTP port of the camera whose IP address is 192.168.0.100 from 80 to 8080, the user must type in the web browser http://192.168.0.100:8080 instead of http://192.168.0.100.
- *RTSP port* – The default setting of the RTSP port is 554. The range is from 1024 to 65535.
- *MJPEG over HTTP port* – The default setting of MJPEG over HTTP port is 8008. The range is from1024 to 65535.

Note:
MJPEG is not supported by Latitude.

- *HTTPS port* – The default setting of HTTPS port is 443. The range is from 1024 to 65535.
- *MTU* – The default setting of the MTU (Maximum Transmission Unit) is the greatest amount of data that can be transferred in one physical frame on the network. For Ethernet, the MTU is 1500 bytes. For PPPoE, the MTU is 1492. The range is from 700 to 1500 bytes.

Note:
Be sure to assign a different port number for each separate service mentioned above.

Click **Save** to save the settings.

IPv6 Address Configuration

With IPv6 support, users can use the corresponding IPv6 address for browsing. Check *Enable IPv6* for to enable this option. Click **Save** to save the settings.

7.3.3.2 QoS (Quality of Service)

QoS provides differentiated service levels for different types of traffic packets and guarantees delivery of priority services during periods of network congestion. Adapting the Differentiated Services (DiffServ) model, traffic flows are classified and marked with DSCP (DiffServ Code point) values, and as a result receive the corresponding forwarding treatment from DiffServ-capable routers.

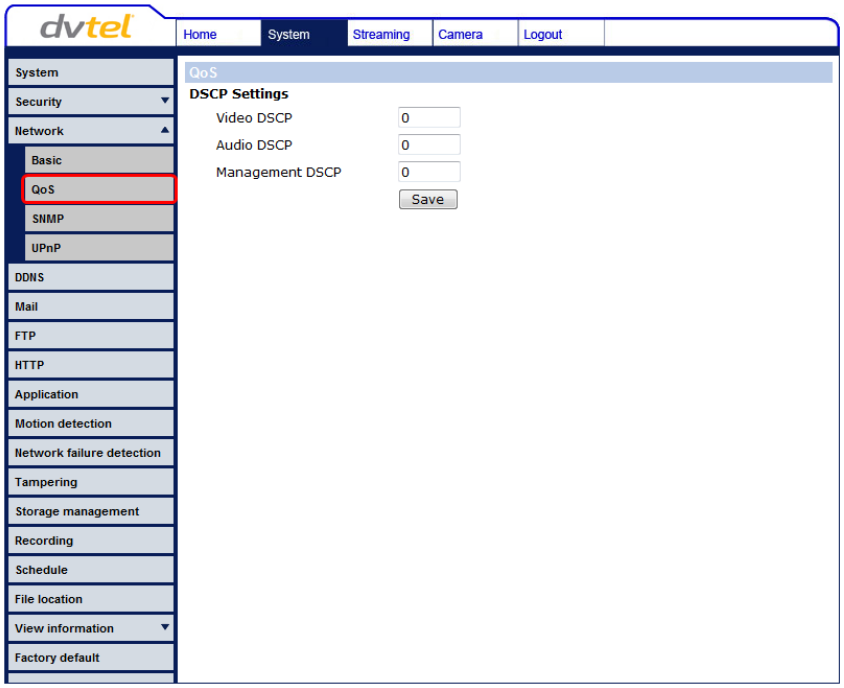


Figure 44: QoS Screen

DSCP Settings

The DSCP value range is from 0 to 63. The default DSCP value is 0 (DSCP disabled). The camera uses the following QoS classes: Video, Audio, and Management.

- *Video DSCP* – This class consists of applications such as MJPEG over HTTP, RTP/RTSP and RTSP/HTTP.

> **Note:**
> MJPEG is not supported by Latitude.

- *Audio DSCP* – The CM-3211/4221 cameras support audio.
- *Management DSCP* – This class consists of HTTP traffic (web browsing).

Click **Save** when complete.

> **Note:**
> To enable this function, make sure the switches/routers in the network support QoS.

7.3.3.3 SNMP Settings

The Simple Network Management Protocol (SNMP) enables the camera to be monitored and managed remotely by the network management system.

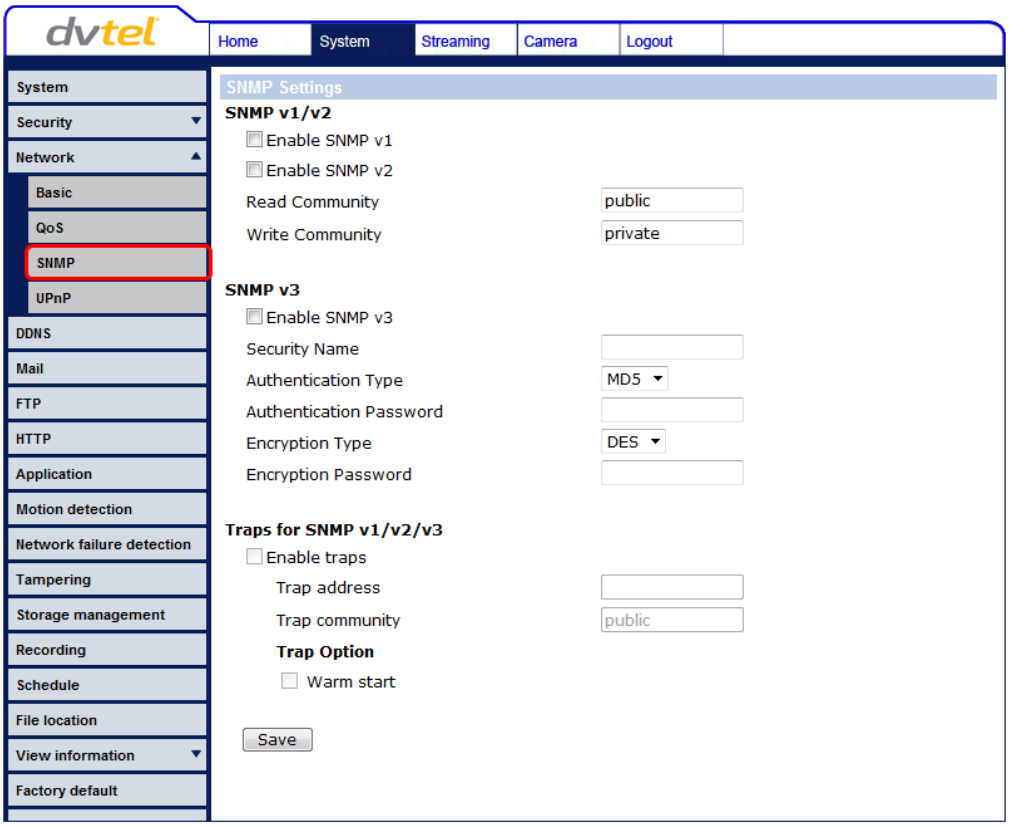


Figure 45: SNMP Settings Screen

SNMP v1/v2

- *Enable SNMP v1* or *Enable SNMP v2* – Select the version of SNMP (v1 or v2) to use by checking the relevant box.
- *Read Community* – Specify the community name that has read-only access to all supported SNMP objects. The default value is *public.*
- *Write Community* – Specify the community name that has read/write access to all supported SNMP objects (except read-only objects). The default value is *private.*

SNMP v3

SNMP v3 provides important security features including:

- Confidentiality – Encryption of packets to prevent snooping by an unauthorized source.
- Integrity – Message integrity to ensure that a packet has not been tampered with in transit including an optional packet replay protection mechanism.
- Authentication – To verify that the message is from a valid source.

To enable the SNMP v3 protocol, enter the appropriate data and passwords requested:

- *Enable SNMP v3* – Select the checkbox.
- *Security Name* – See note below.
- *Authentication Type* – Select MD5 or SHA from the drop-down menu. See note below.
- *Authentication Password* – See note below.
- *Encryption Type* – either DES or AES. See note below.
- *Encryption Password* – See note below.

Note:
You may have to consult with your System Administrator to activate this function.

Traps for SNMP v1/v2/v3

Traps are used by the camera to send messages to a management system for important events or status changes.

- *Enable traps* – Check this box to activate trap reporting.
  - *Trap address* – Enter the IP address of the management server.
  - *Trap community* – Enter the community to use when sending a trap message to the management system. The default value is *public*.
- Trap Option
  - *Warm start* – A warm start SNMP trap signifies that the SNMP device, such as the camera, performs a software reload.

Click **Save** when complete.

7.3.3.4 UPnP

The **UPnP** page enables the Universal Plug-and-Play protocol on your network devices.

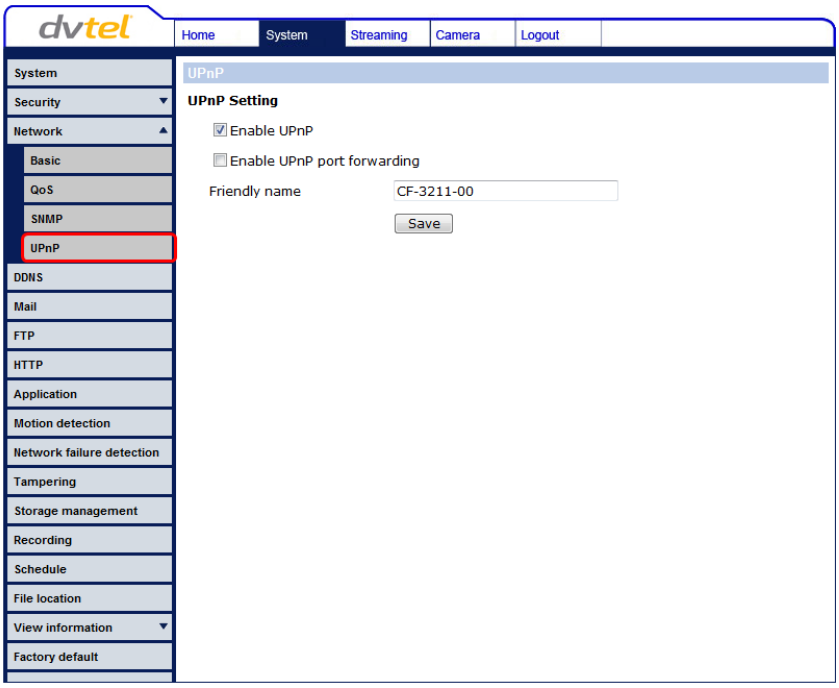


Figure 46: UPnP Screen

UPnP Settings

- *Enable UPnP* – If UPnP is enabled and a camera is discovered on the LAN, the icon of the connected camera appears in **My Network Places**, allowing direct access, as seen below.

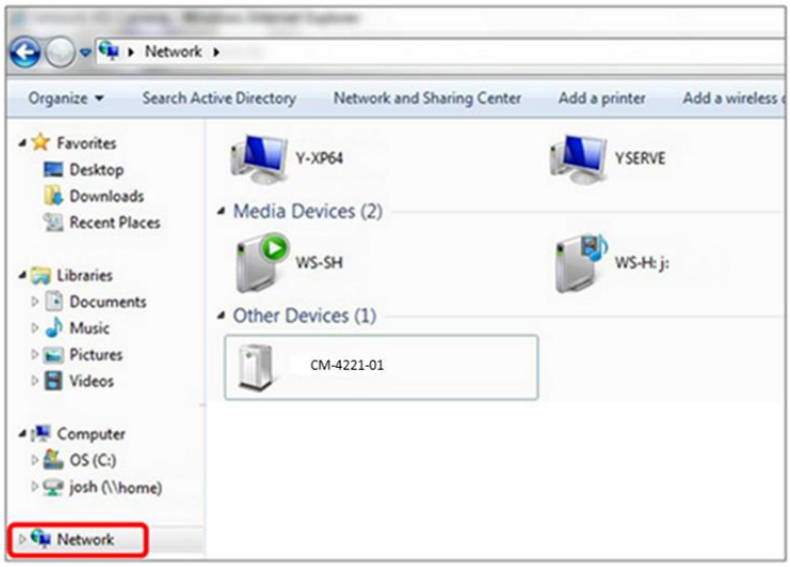


Figure 47: Direct Access to Camera with UPnP Enabled

Note:
To enable this function, make sure the UPnP component is installed on your computer. Refer to Install UPnP Components for the Windows 7 and Windows 8 procedure.

- *Enable UPnP port forwarding* – When UPnP port forwarding is enabled, the camera is allowed to open the web server port on the router automatically.

> **Note:**
> To enable this function, make sure that your router supports UPnP and that it is activated.

- *Friendly name* – Set the name for the camera for identification.

Click **Save** to save the settings.

7.3.4 DDNS

Dynamic Domain Name System (DDNS) allows a host name to be constantly synchronized with a dynamic IP address. This permits those using a dynamic IP address to be accessed by a static domain name.

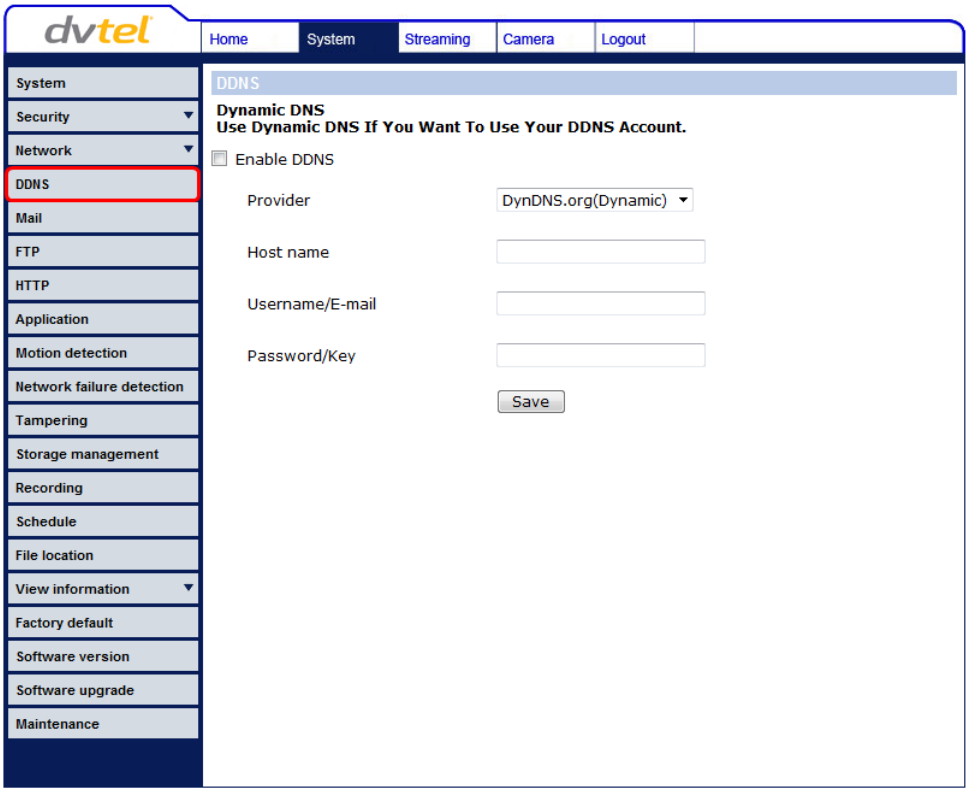


Figure 48: DDNS Screen

Enable DDNS

Check this box to enable DDNS.

- *Provider* – Select a DDNS host provider name from the drop-down menu.
- *Host name* – Enter the registered domain name in the field.
- *Username/E-mail* – Enter the username or e-mail address required by the DDNS provider for authentication.
- *Password/Key* – Enter the password or key required by the DDNS provider for authentication.

Click **Save** to save the setting.

7.3.5 Mail

The Administrator can send an e-mail via Simple Mail Transfer Protocol (SMTP) when an alarm is triggered SMTP is a protocol for sending e-mail messages between servers. SMTP is a relatively simple, text-based protocol, where one or more recipients of a message are specified and the message text is transferred.

Two SMTP server accounts can be configured. Settings include SMTP Server, account name, password, and e-mail address settings. Enter the details in the appropriate fields. For SMTP server details, contact your network service provider. Click **Save** when finished. The following screen shows the SMTP configuration.

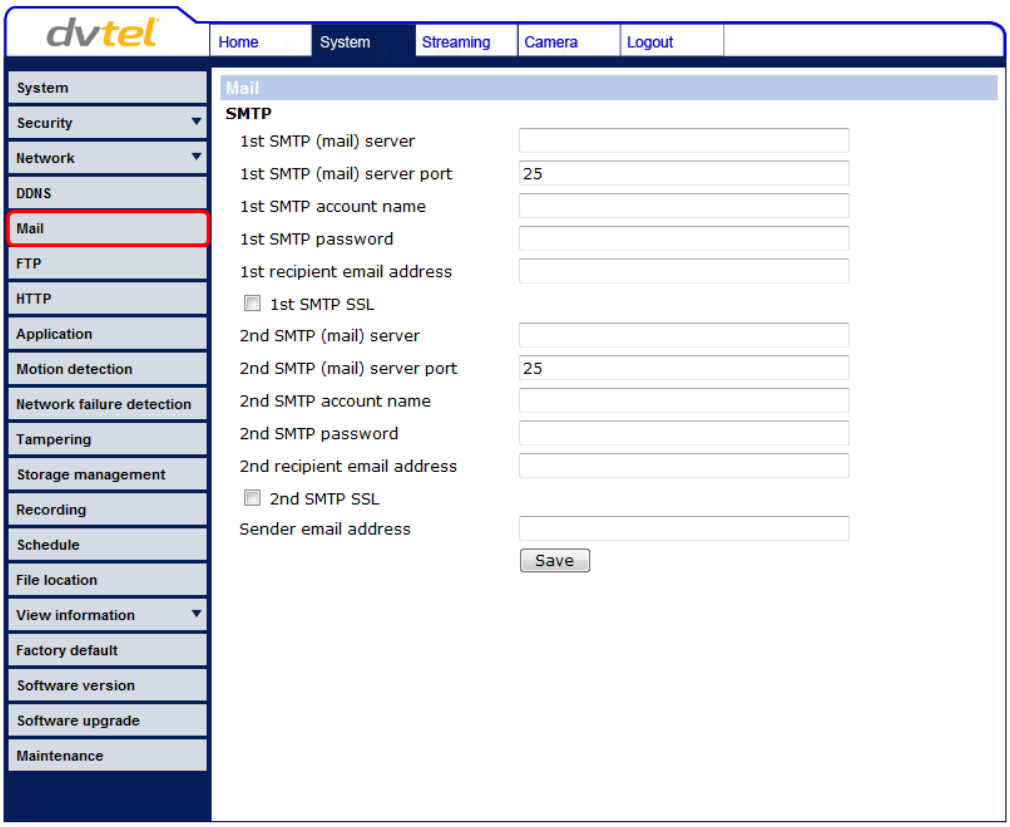


Figure 49: Mail Screen – SMTP

7.3.6 FTP

The Administrator can send an alarm message to one or two File Transfer Protocol (FTP) sites when motion is detected. Settings include first and second server, server port, user name, password, and remote folder. Enter the details in the appropriate fields. Click **Save** when finished. The following screen shows the FTP settings.

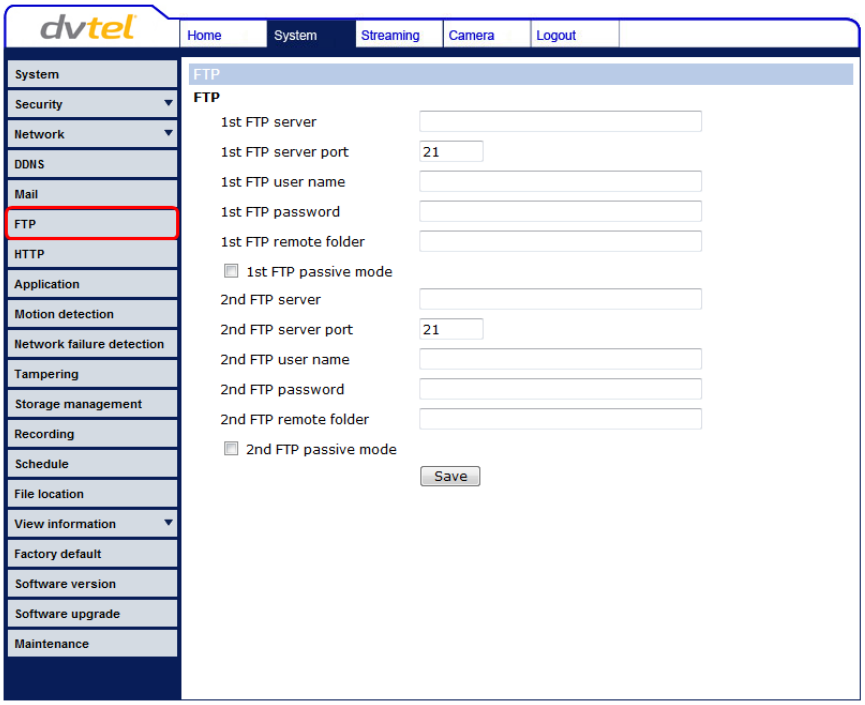


Figure 50: FTP Screen

7.3.7 HTTP

An HTTP notification server detects notification messages of triggered events sent from cameras. Two notification server accounts (Alarm Triggered and Motion Detection**)** can be set up and sent to the specified HTTP servers. Enter the HTTP details, including server, user name, and password, in the appropriate fields. Click **Save** when finished. The settings are displayed in the **HTTP** screen below.

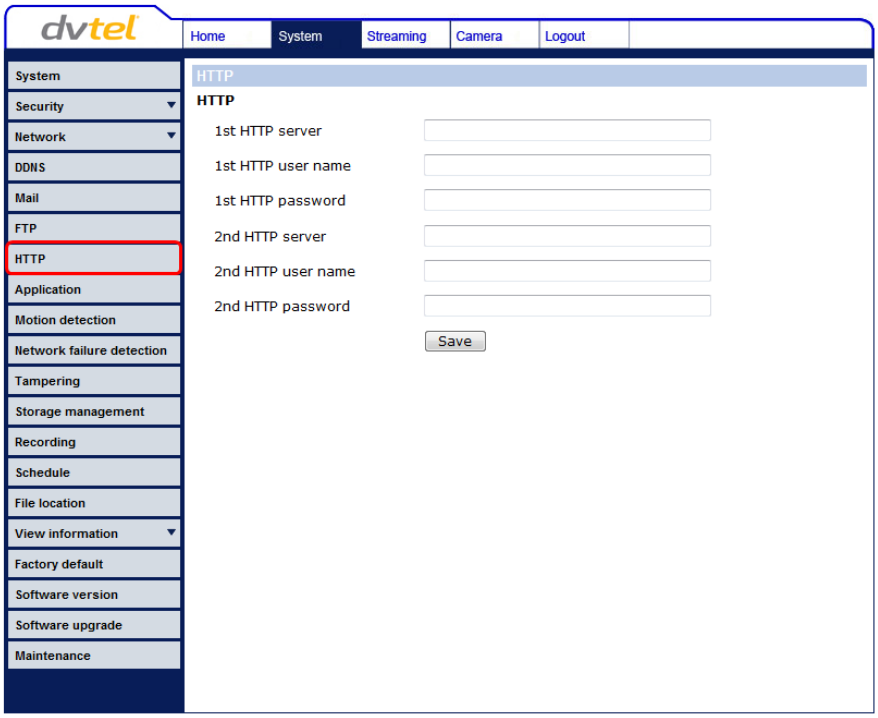


Figure 51: HTTP Screen

Refer to *Send HTTP notification* and *Motion Detection* for HTTP notification settings in the Application section below.

7.3.8 Application

The **Application** screen enables control over the input and output alarms. If, for example, an event is recognized by the system, an input or output alarm and message is generated.

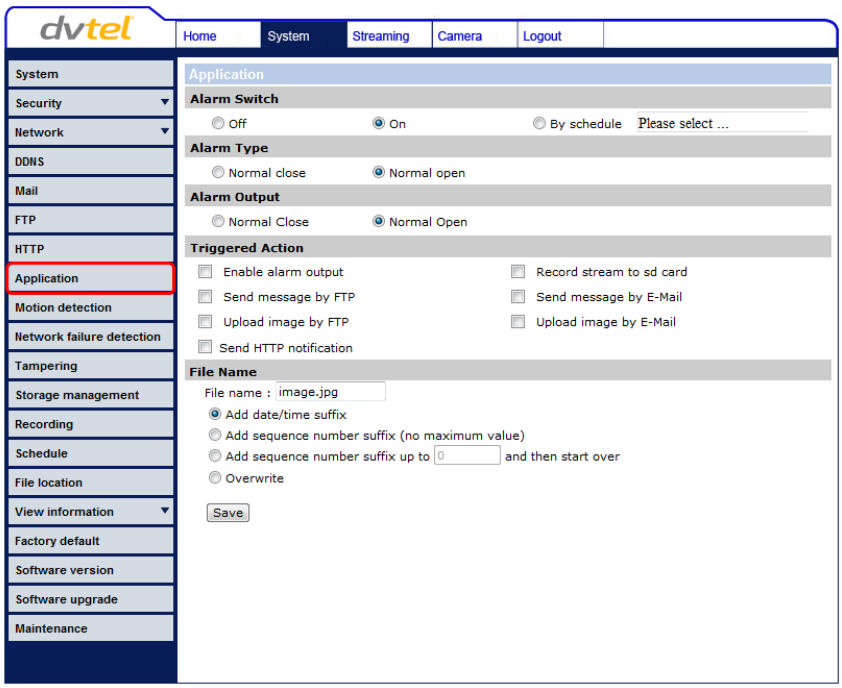
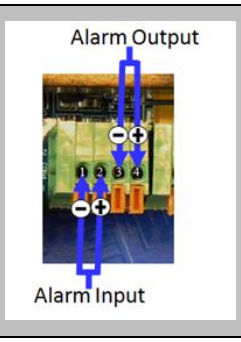


Figure 52: Application Screen

The alarm input and output connectors are shown in the table below.

Table 5: Input/Output Alarm Connections

Pin No.	Designation
1	Input (-)
2	Input (+)
3	Output (-)
4	Output (+)



Alarm Switch

The Administrator can enable or disable the alarm function (*Off/On*).

Alarm Type

Select an alarm type (*Normal close* or *Normal open*) that corresponds to the alarm application.

Alarm Output

Define the normal alarm output signal as *Normal Close* or *Normal Open*, according to the current alarm application.

Triggered Action

The Administrator can specify various alarm actions to be taken when an alarm is triggered. The options are listed below.

- *Enable alarm output* – Select this box to enable alarm relay output.
- *Record stream to sd card* – Select this box in order to save the alarm-triggered recording to your microSD/SDHC card. Enter the number of seconds for the pre-trigger buffer. Select the first radial button if you wish to upload for a specified length of time and enter the number of seconds. Alternatively, select the second radial button to upload during the active trigger. See Figure 53: Application – Record Stream to SD Card.

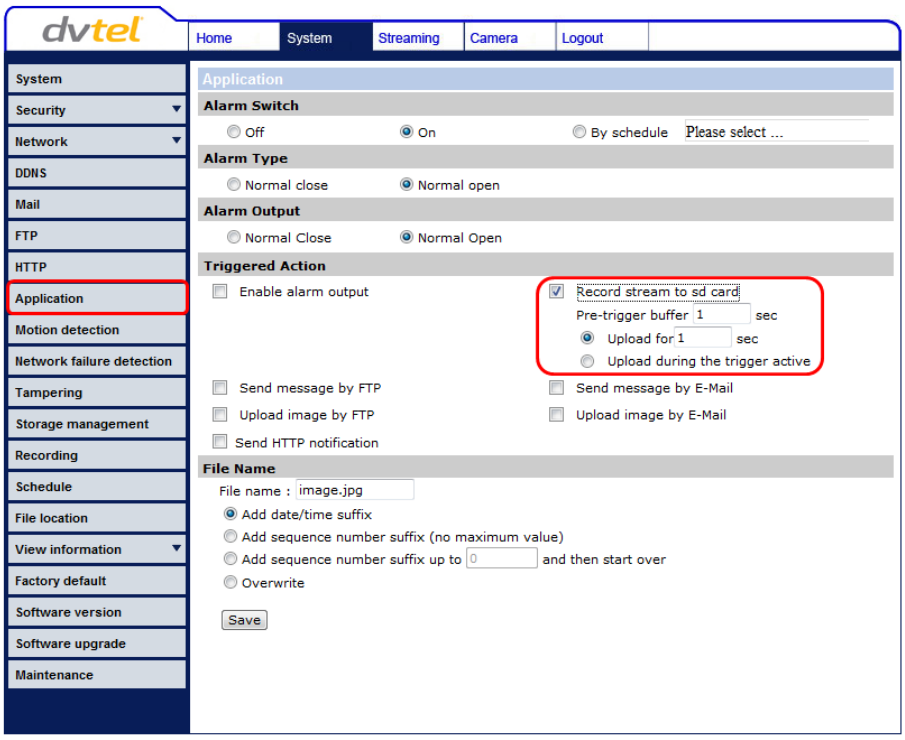


Figure 53: Application – Record Stream to SD Card

Note:
Make sure that local recording (with a microSD/SDHC card) is activated so that this function can be implemented. See Recording for further details.

- *Send Message by FTP/E-Mail* – Select whether to send an alarm message by FTP and/or e-mail when an alarm is triggered.

- *Upload Image by FTP* – As seen in the figure below, select this box to assign an FTP site and configure the parameters shown. When an alarm is triggered, event images are uploaded to the designated FTP site. Specify which one of two FTP addresses you wish to use from the drop-down menu. Select the number of frames for the pre-trigger and post-trigger buffers from the drop-down menu of 1-20 frames.

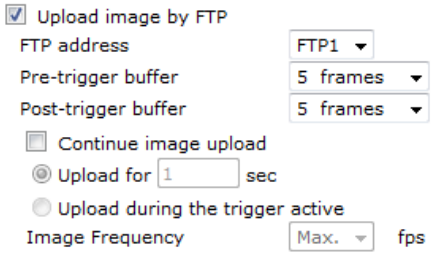


Figure 54: Application – Upload Image by FTP

Check the *Continue image upload* box if you wish to use this option. If you wish to specify the length of time for the upload, click on this radial button and enter the number of seconds. If you wish to upload during the active trigger, click on this radial button.

Finally, select the number of frames per second from the drop-down menu next to *Image frequency.*

- *Upload Image by E-Mail* – Select this box in order to assign an e-mail address and configure various parameters as shown in the figure below. When the alarm is triggered, event images are sent to one of two designated e-mail addresses. Select the number of frames for the pre-trigger and post-trigger buffers from the drop-down menu of 1-20 frames. See Figure 55: Application – Upload Image by E-Mail.

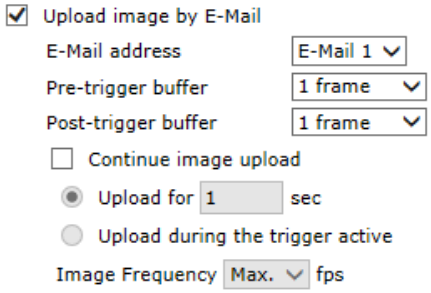


Figure 55: Application – Upload Image by E-Mail

Check the box for *Continue image upload* if you wish to use this option. If you wish to specify the length of time for the upload, click on this radial button and enter the number of seconds. If you wish to upload during the active trigger, click on this radial button.

Finally, select the number of frames per second from the drop-down menu next to *Image frequency.*

Note:
Make sure that SMTP or FTP configuration has been completed. See Mail and FTP for further details.

- *Send HTTP notification* – Check this box to specify the destination HTTP address and parameters for event notifications by the triggered alarm. When an alarm is triggered, the notification will be sent to one of two specified HTTP servers. See figure below.

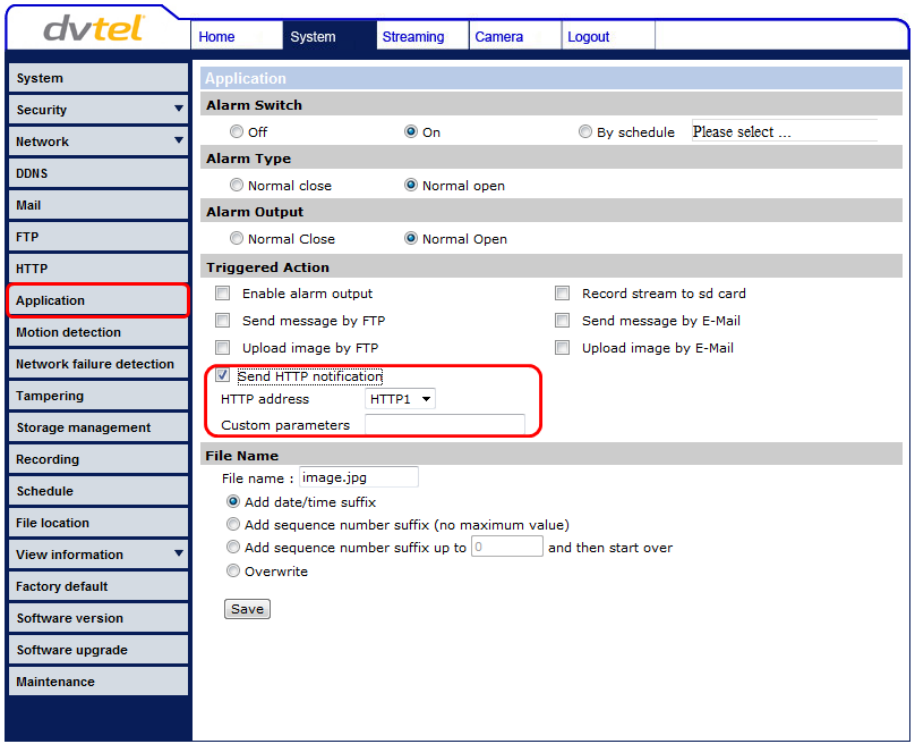


Figure 56: Application – Send HTTP Notification

File Name

- *File Name* – Enter a file name in the field, for example *image.jpg.* The uploaded image's file name format is set in this section. Select one that meets your requirements.

  - Add date/time suffix
    File name: imageYYMMDD_HHNNSS_XX.jpg
    Y: Year, M: Month, D: Day
    H: Hour, N: Minute, S: Second
    X: Sequence Number

  - Add sequence number suffix (no maximum value)
    File name: imageXXXXXXX.jpg
    X: Sequence Number

  - Add sequence number suffix (limited value)
    File Name: imageXX.jpg
    X: Sequence Number

    The file name suffix ends at the number being set. For example, if the setting is up to "10," the file name will start from 00, end at 10, and then start over again.

  - Overwrite
    The original image in the FTP site will be overwritten by the new uploaded file with a static filename.

After entering all the settings, click **Save**.

7.3.9 Motion Detection

The motion detection function detects suspicious motion and triggers alarms when motion volume in the detected area reaches/exceeds the determined sensitivity threshold value.

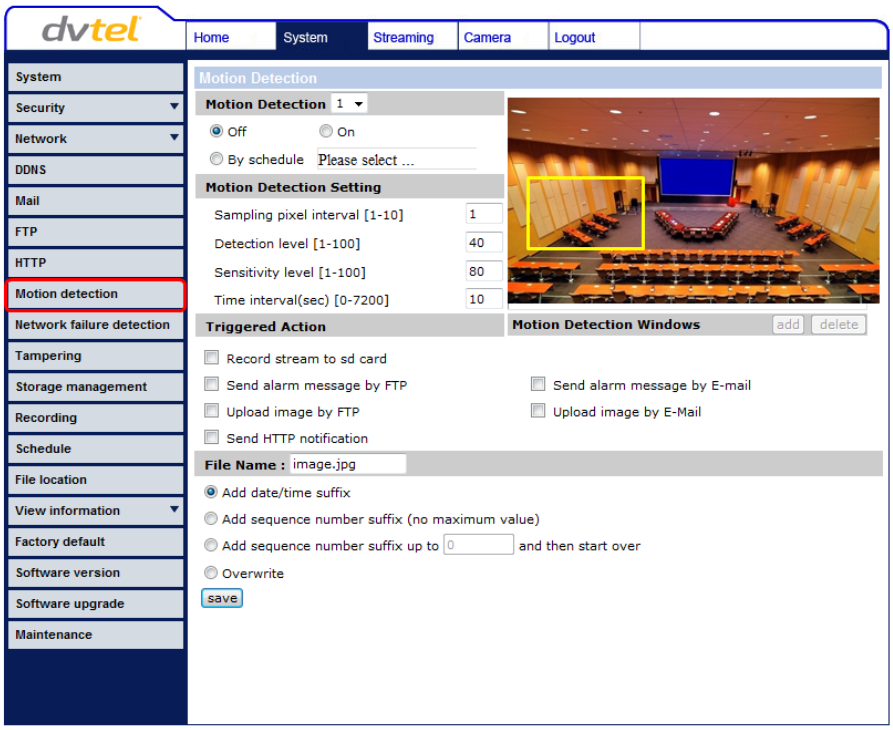


Figure 57: Motion Detection Screen

Within the Live View pane on the **Motion Detection** screen, there is a frame (**Motion Detection** window) which is used for defining the motion detection area. To change the size of the **Motion Detection** window, move the mouse cursor to the edge of the frame and drag it outward/inward. Moving the mouse to the center of the frame shifts the frame to the intended location.

Motion Detection Activation

The motion detection function may be turned on or off in the **Motion Detection** screen. The default setting is *Off*.

By Schedule

To set a schedule:

1. Select *By schedule*.
2. Click *Please Select.* A drop-down menu opens.
3. From the drop-down menu, select a schedule from 1 to 10.

For instructions how to set a schedule for motion detection, refer to Schedule. Below is a screen showing the *Schedule* drop-down menu with selected schedules.

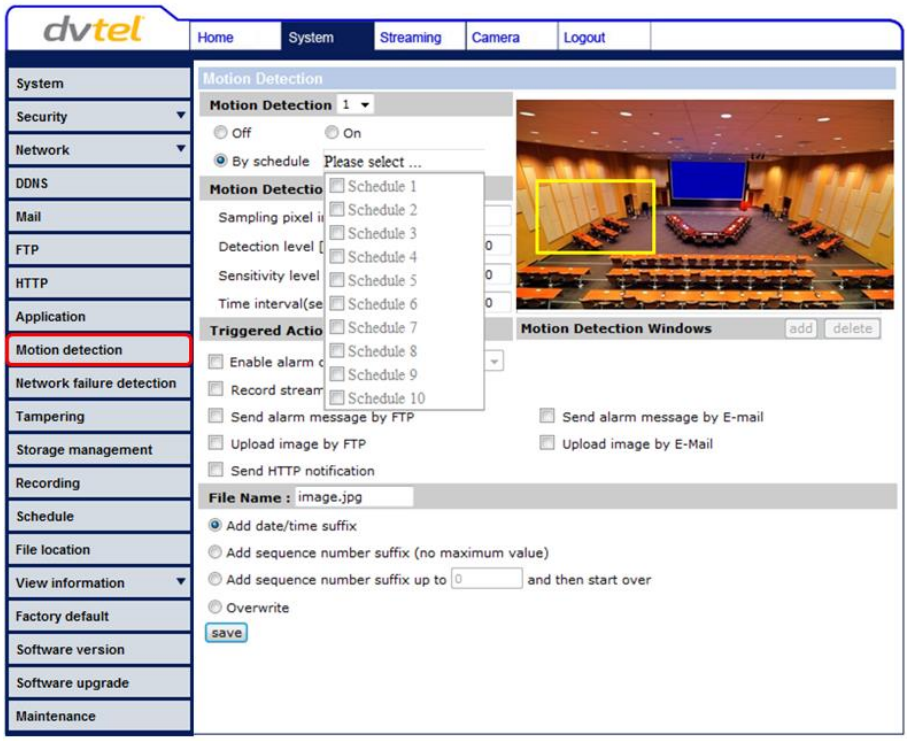
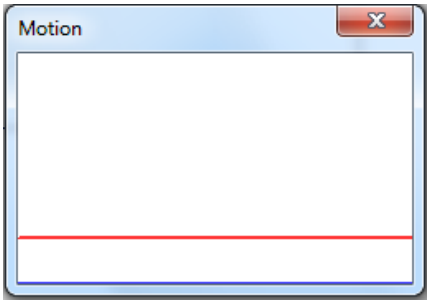


Figure 58: Motion Detection Screen – with Schedule Drop-Down Menu

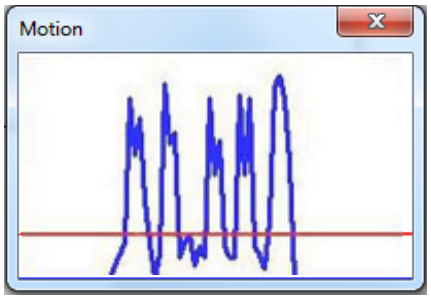
Motion Detection Windows

Up to 10 **Motion Detection** windows can be set. Press the **add** button under the Live View pane to add a **Motion Detection** window. To cancel a **Motion Detection** window, move the mouse cursor to the selected window and click **delete**.

If the motion detection function is activated, the following **Motion** pop-up window appears.

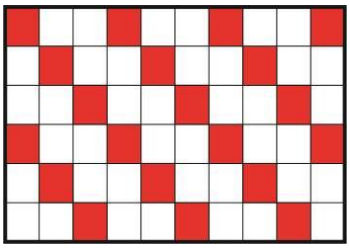


When motion is detected, the signals are displayed in the **Motion** window shown below.



Detailed settings for motion detection are as follows:

- *Sampling pixel interval* [*1-10]* – Select a number from 1-10. The default value is 1. If the value is set as 3, within the detection region, the system will take one sampling pixel for every 3 pixels by each row and each column (see the figure below).



- *Detection level* [*1-100]* – Select a number from 1-100. The default level is 40. This sets detection level for each sampling pixel; the smaller the value, the more sensitive it is.
- *Sensitivity level [1-100]* – Select a number from 1-100. The default level is 80, which means if 20% or more sampling pixels are detected differently, the system will detect motion. The bigger the value, the more sensitive it is. When the value is bigger, the red horizontal line in the motion indication window will be lowered accordingly.
- *Time interval (sec) [0-7200]* – Select a number from 0-7200 (seconds). The default interval is 10. The value is the interval between each detected motion.

Triggered Action

The Administrator can specify alarm actions to be taken when motion is detected. See Figure 57: Motion Detection Screen. The options are listed as follows:

- *Enable alarm output* – Check this box and select the predefined type of alarm output *(low* or *high*) to enable alarm relay when tampering is detected.
- *Record stream to sd card* – Select this box to store the motion detection alarm recording in a microSD/SDHC card when tampering is detected. Enter the number of seconds for the pre-trigger buffer. Select the first radial button to upload for a specified length of time and enter the number of seconds. Alternatively, select the second radial button to upload during the active trigger. See Figure 53: Application – Record Stream to SD Card.

> **Note:**
> Make sure the local recording (with microSD/SDHC card) is activated so that this function can be implemented. See Recording for further details.

- *Send Message by FTP/E-Mail* – Select whether to send an alarm message by FTP and/or e-mail when motion is detected.

- *Upload Image by FTP* – Select this box in order to upload an image to a designated FTP site when motion is detected according to various parameters, as seen in Figure 54: Application – Upload Image by FTP. Specify the FTP address to use from the drop-down menu. Select the number of frames for the pre-trigger and post-trigger buffers from the drop-down menu of 1-20 frames.

  Check the box for *Continue image upload* if you wish to use this option. To specify the length of time for the upload, click on this radial button and enter the number of seconds. To upload during the active trigger, click on this radial button. Finally, select the number of frames per second from the drop-down menu next to *Image frequency*.

- *Upload Image by E-Mail* – Select this box in order to assign an e-mail address and configure various parameters, as seen in Figure 55: Application – Upload Image by E-Mail. When motion is detected, event images are sent to one of two designated e-mail addresses. Select the number of frames for the pre-trigger and post-trigger buffers from the drop-down menu of 1-20 frames.

  Check the box for *Continue image upload* to use this option. To specify the length of time for the upload, click on this radial button and enter the number of seconds. To upload during the active trigger, click on this radial button. Finally, select the number of frames per second from the drop-down menu next to *Image frequency.*

  Note:
  Make sure that SMTP or FTP configuration has been completed. See Mail and FTP for further details.

- *Send HTTP notification* – Check this box to send a notification by HTTP. Select the destination HTTP address from the drop-down menu and specify the parameters for event notifications by motion detection triggered. When an alarm is triggered, the notification will be sent to one of two specified HTTP servers. See Figure 56: Application – Send HTTP Notification.

  Note:
  Make sure that local recording (with a microSD/SDHC card) is activated so that this function can be implemented. See Recording for further details.

File Name

The uploaded image's filename format is set in this section. Select one that meets your requirements.

Save

Click **Save** to save the motion detection settings.

7.3.10 Network Failure Detection

The network failure detection function allows the IP camera to periodically ping another IP device within the network to detect a network failure, for example, if a video server is disconnected. By implementing local recording (through a microSD/SDHC card) if a network failure occurs, the camera can operate as a backup recording device for the surveillance system.

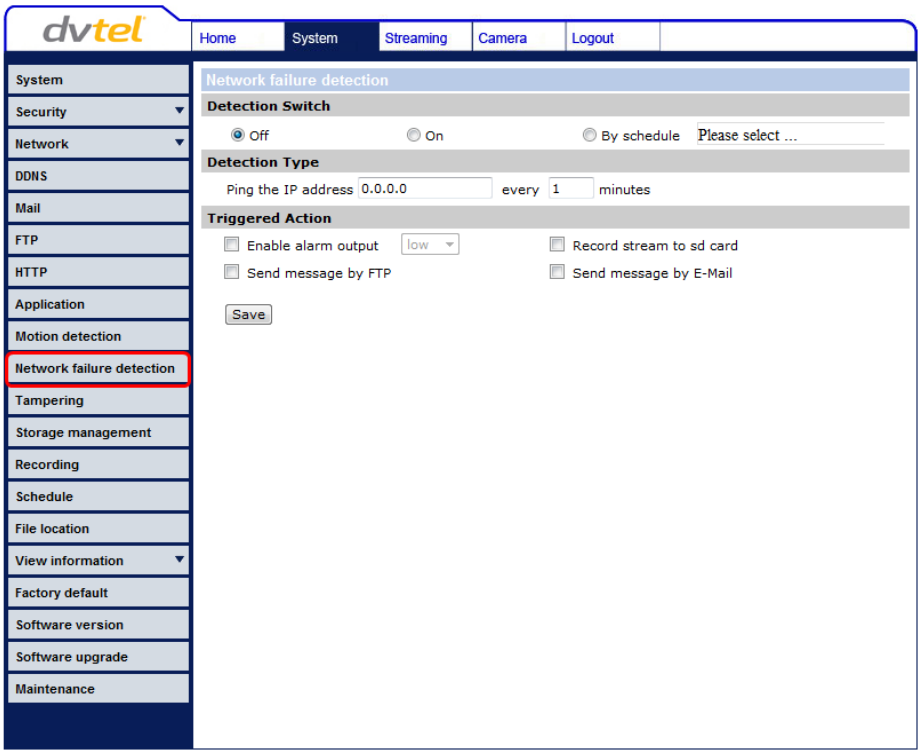


Figure 59: Network Failure Detection Screen

Detection Switch

The Administrator can enable or disable the detection function by selecting *On* or *Off*.

By Schedule

To set a schedule:

1. Select *By schedule*.
2. Click *Please Select.* A drop-down menu opens.
3. From the drop-down menu, select a schedule from 1 to 10.

For instructions how to set a schedule, refer to Schedule.

Detection Type

In the text box, enter the IP address to ping and the time interval in minutes between pings.

Triggered Action

The Administrator can specify various alarm actions to be taken when an alarm is triggered. The options are listed below.

- *Enable alarm output* – Check this box and select the predefined type of alarm output *(low* or *high*) to enable alarm relay when tampering is detected.
- *Record stream to sd card* — Select this box in order to save the alarm-triggered recording into a microSD/SDHC card. Enter the number of seconds for the pre-trigger buffer. Select the first radial button to upload for a specified length of time and enter the number of seconds. Alternatively, select the second radial button to upload during the active trigger. See Figure 53: Application – Record Stream to SD Card.

> **Note:**
> Make sure that local recording (with a microSD/SDHC card) is activated so that this function can be implemented. See Recording for further details.

- *Send message by FTP/E-Mail* – Select whether to send an alarm message by FTP and/or e-mail when a network failure is detected.

Save

Click **Save** to save the network failure detection settings.

7.3.11 Tampering

The tampering alarm function helps the IP camera deal with tampering (such as, deliberate redirection, blocking, paint-spraying, and obscuring the lens, etc.). Using video analysis, the camera can react to such events by sending out notifications or uploading snapshots to the specified destination(s).

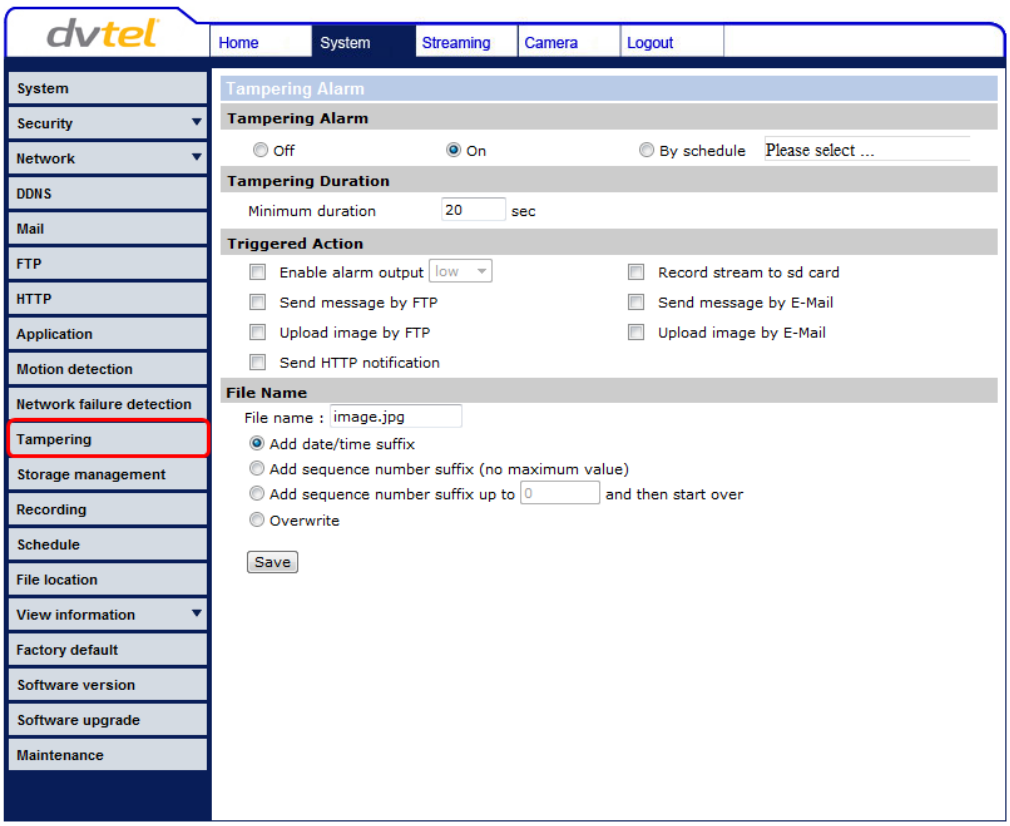


Figure 60: Tampering Alarm Screen

Detection of camera tampering is achieved by measuring the differences between the older frames of video (which are stored in buffers) and more recent frames.

Tampering Alarm

The tampering alarm function may be turned on or off in the **Tampering Alarm** page. The default setting is *Off.*

By Schedule

To set a schedule:

1. Select By schedule.
2. Click *Please Select.* A drop-down menu opens.
3. From the drop-down menu, select a schedule from 1 to 10.

For instructions how to set a schedule, refer to Schedule.

Tampering Duration

Minimum tampering duration is the time for video analysis to determine whether camera tampering has occurred. Minimum duration could also be interpreted as defining the tampering threshold; a longer duration represents a higher threshold. The tampering duration time range is from 10 to 3600 seconds.

Triggered Action

The Administrator can specify multiple alarm actions to be taken when tampering is detected. All options are listed as follows:

- *Enable alarm output* – Check this box and select the predefined type of alarm output *(high* or *low*) to enable alarm relay when tampering is detected.
- *Record stream to sd card* – Select this box in order to save the alarm-triggered recording into a microSD/SDHC card. Enter the number of seconds for the pre-trigger buffer. Select the first radial button to upload for a specified length of time and enter the number of seconds. Alternatively, select the second radial button to upload during the active trigger. See Figure 53: Application – Record Stream to SD Card.

  Note:
  Make sure the local recording (with a microSD/SDHC card) is activated so that this function can be implemented. See Recording for further details.

- *Send Alarm Message by FTP/E-Mail* – The Administrator can select whether to send an alarm message by FTP and/or E-Mail when tampering is detected.
- *Upload Image by FTP* – Selecting this option enables you to assign an FTP site and configure various parameters, as shown in Figure 54: Application – Upload Image by FTP. When tampering is detected, event images will be uploaded to the designated FTP site. Specify the FTP address to use from the drop-down menu. Select the number of frames for the pre-trigger and post-trigger buffers from the drop-down menu of 1-20 frames.

  Check the box for *Continue image upload if* you wish to use this option. To specify the length of time for the upload, click on this radial button and enter the number of seconds. To upload during the active trigger, click on this radial button.

  Finally, select the number of frames per second from the drop-down menu next to *Image frequency*.

- *Upload Image by E-Mail* – Selecting this option enables you to assign an e-mail address and configure various parameters, as shown in Figure 55: Application – Upload Image by E-Mail. When tampering is detected, event images will be sent to the designated e-mail address.

  Specify two e-mail addresses to use from the drop-down menu. Select the number of frames for the pre-trigger and post-trigger buffers from the drop-down menu of 1-20 frames.

  Check the box for *Continue image upload* if you wish to use this option. To specify the length of time for the upload, click on this radial button and enter the number of seconds. To upload during the active trigger, click on this radial button. Finally, select the number of frames per second from the drop-down menu next to *Image frequency.*

  Note:
  Make sure SMTP or FTP configuration has been completed. See section Mail and FTP for further details.

- *Send HTTP notification* – Check this option, select the destination HTTP address, and specify the parameters for HTTP notifications. When the tampering alarm is triggered, the HTTP notifications can be sent to the specified HTTP server. See Figure 56: Application – Send HTTP Notification.

File Name

The uploaded image's filename format can be set in this section. Select the one that meets your requirements.

Save

Click **Save** to save all the specified tampering alarm settings.

7.3.12 Storage Management

You can locally record up to 32GB on a microSD/SDHC card. The **Storage Management** page shows the capacity information of the card and a recording list of all the recording files saved on the memory card. You can also format the card and implement automatic recording cleanup on this page. To implement microSD/SDHC card recording, see Recording.

Note:
Format the microSD/SDHC card when using it for the first time. Formatting is also required when a memory card has been used on one camera and is then transferred to a camera that uses a different software platform.

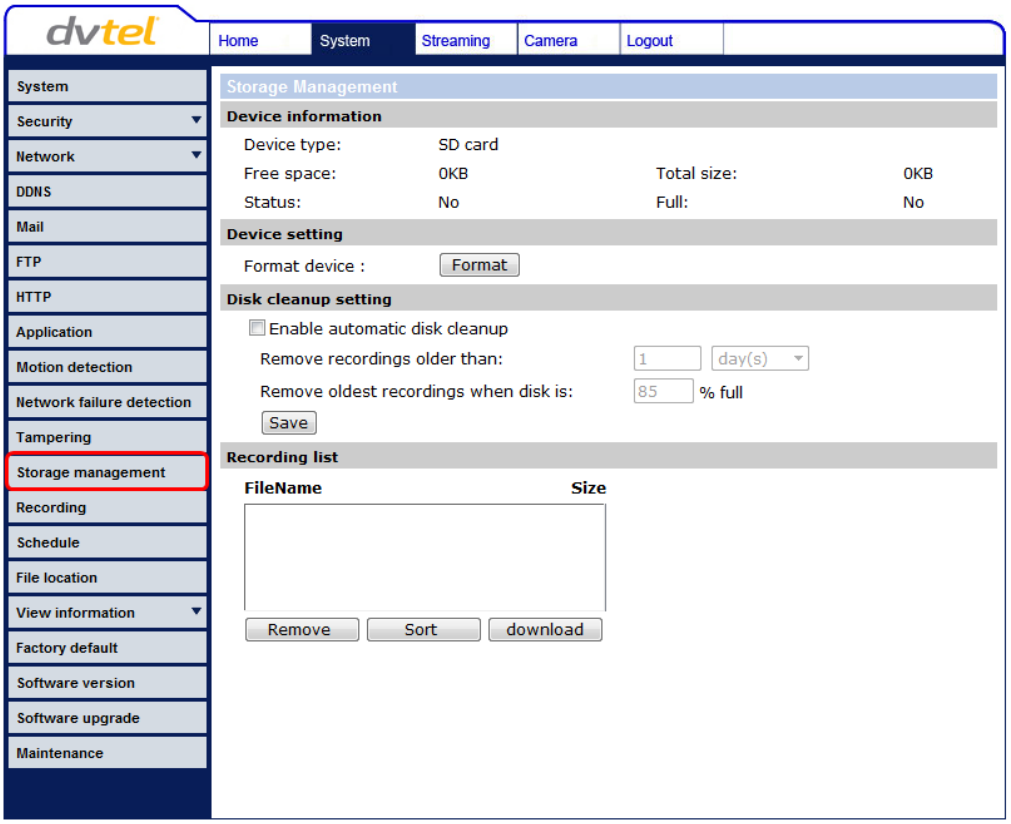


Figure 61: Storage Management Screen

Device information

Upon inserting the microSD/SDHC card, card information, such as the memory capacity and status, is displayed.

Device setting

Click **Format** to format the memory card.

Disk cleanup setting

Enable automatic recording cleanup by selecting *Enable automatic disk cleanup*. From the pull-down menu, specify the minimum length of time over which to remove recordings. For example, remove recordings over 10 days old. Enter the percent of disk capacity used in order to remove the oldest recordings. Click **Save** when finished.

Recording List

Each video file on the microSD/SDHC card is listed in the Recording list below. The maximum file size is 60 MB per file. See Recording for further details.

When the recording mode is set as *Always* (consecutive recording) and the microSD/SDHC card recording is enabled by events triggered, the system immediately saves a recorded event on the memory card once an event occurs. Then the camera will return to the regular recording mode after events recording.

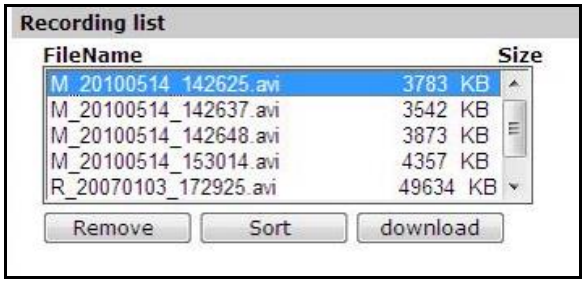


Figure 62: Video File Recording List

- *Remove* – To remove a file, first select the file and then click **Remove**.
- *Sort* – Click **Sort** to list the files in the Recording list in order of name and date.

Note:
The capital letters: R, N, A, (A0), M, (M0) followed by an underscore, appear at the beginning of the file name. They denote the type of recording.

- R - Regular (always or schedule)
- N - Network failure
- M - Motion, (M0 refers to the first motion window trigger)
- A - Alarm (A0 refers to the first alarm trigger input).

- *Download* – To open/download a video clip, first select the file and then click **download**. The selected file window pops up as shown below. Click on the AVI file to play the video in the player or download it to a specified location.

Figure 63: Selected File Window

7.3.13 Recording

In the **Recording** screen, specify the recording schedule. Select one of three options:

- *Disable* – Disable this function
- *Always* – Always use this function
- *Only during time frame* – Records only during a specified time frame

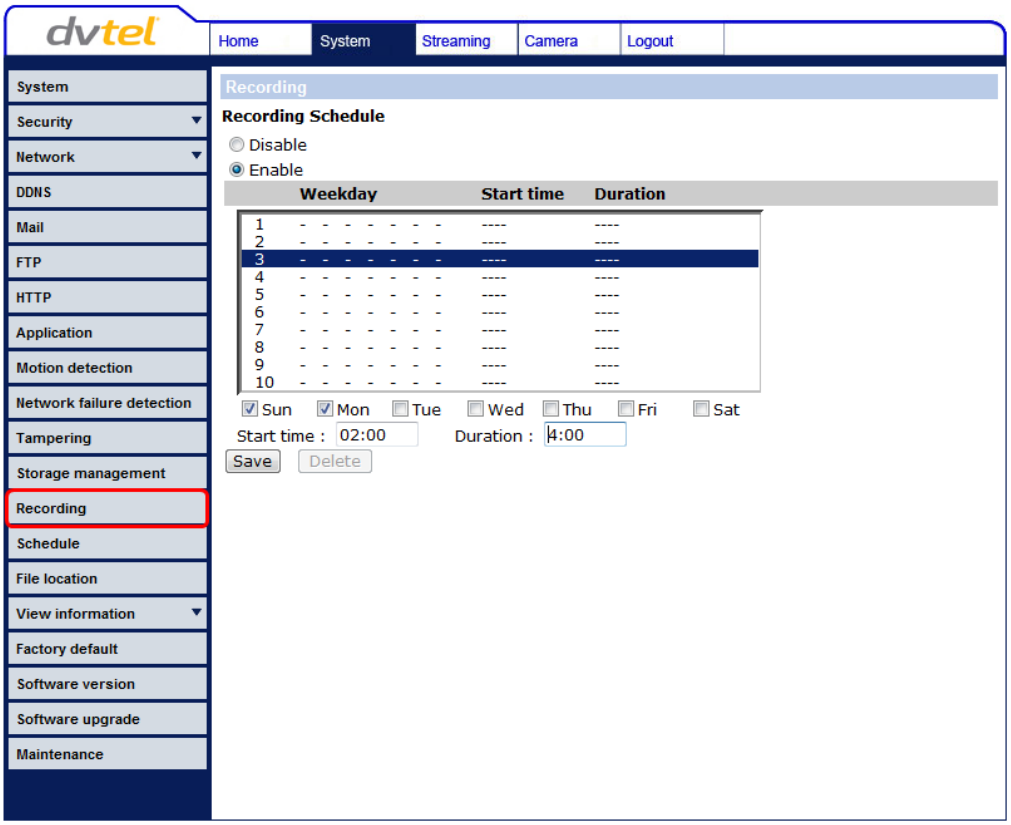


Figure 64: Recording Screen

Activating microSD/SDHC card recording

Two types of schedule mode are available: *Always* and *Time Frame setting*. You can setup the time frame to fit the recording schedule by selecting the day(s), start time and duration for recording. Choosing *Always* activates the microSD/SDHC card recording all the time. Click **Save** to confirm the schedule mode.

Terminating microSD/SDHC card recording

Select *Disable* to terminate the recording function.

Note:
This option works only if the microSD/SDHC card is installed in the camera.

7.3.14 Schedule

The **Schedule** screen is used by the network failure detection, tampering and motion detection functions. To access the schedule function, open the **Main** window, select the **System** tab, and click on the **Schedule** tab. The functions in this tab allow administrators to create customized schedules for the camera using this option. If a schedule exists, the administrator can apply that schedule to this camera using the available dropdown. See Figure 65: Schedule Screen.

Note:
This application is not the same as the Recording Schedule function.

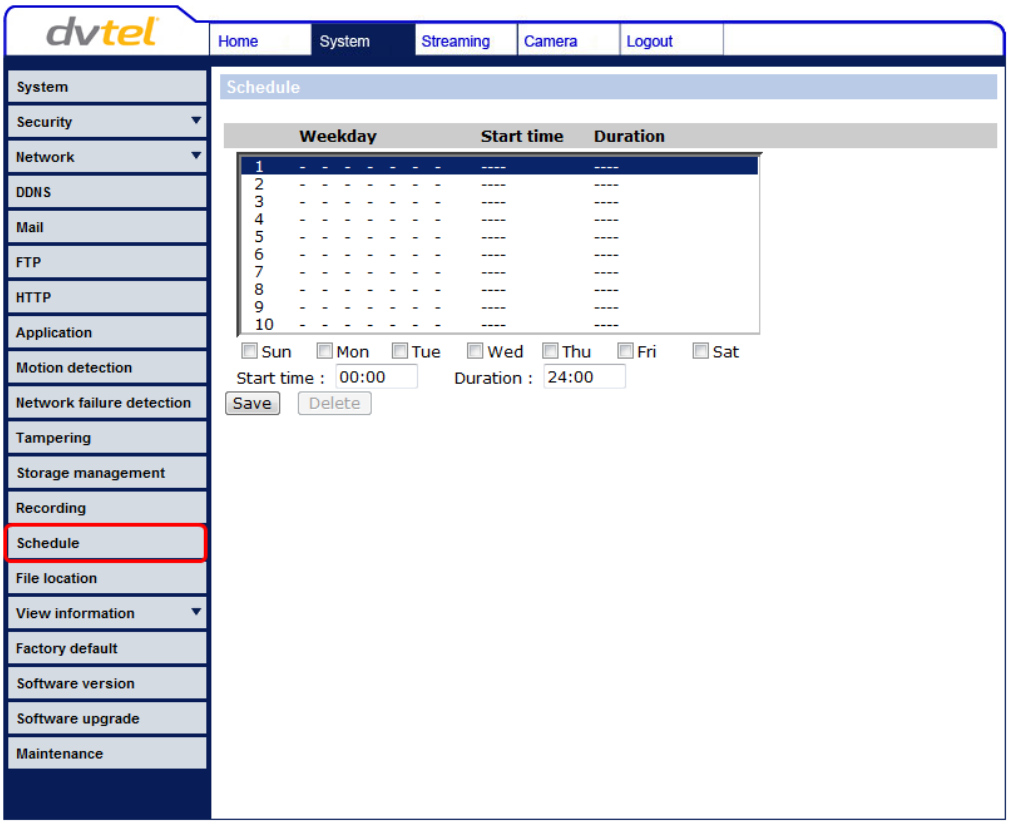


Figure 65: Schedule Screen

To create a new schedule or edit an existing schedule:

1. Click on the appropriate checkboxes relating to the days of the week (Sun, Mon, Tue, Wed, Thu, Fri and Sat) to create a schedule. Tuesday (Tue) is checked in the example. See Figure 65.
2. Set Start time (for example, 09:00) and Duration (for example, 4:00 hours).
3. Click Save to apply the newly created schedule to the camera.

Removing Schedules

1. To remove a schedule, select the setup data line by line.
2. Click **Delete** to remove.

7.3.15 File Location

From the **File Location** page, specify a storage location for snapshots and web recordings. The default setting is: C:\. After confirming the setting, click **Save** to save the snapshots and recordings in the designated location.

Note:
Make sure the selected file path contains valid characters.

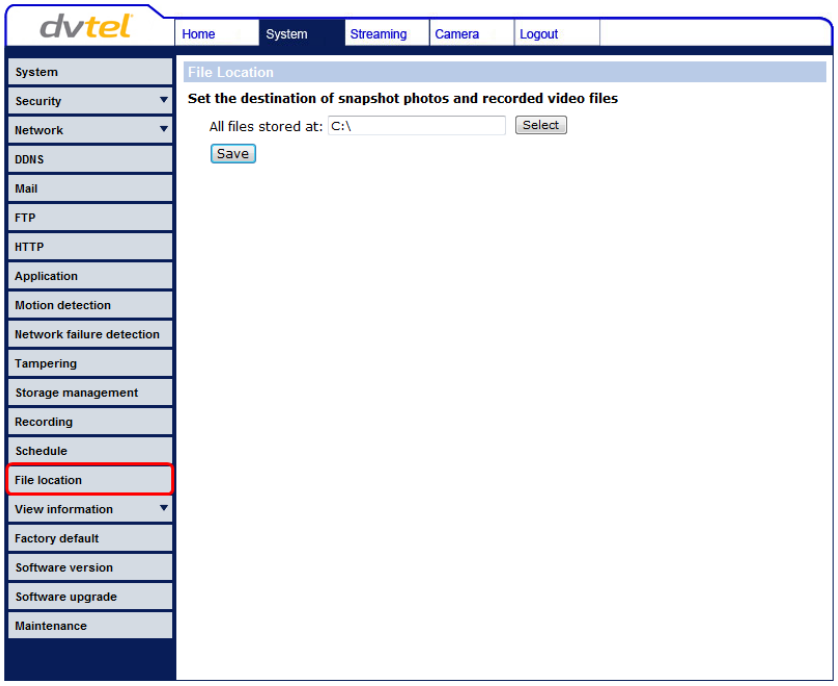


Figure 66: File Location Screen

7.3.16 View Information

Clicking the **View Information** tab in the **System** screen opens a drop-down menu with tabs **Log File**, **User Information**, and **Parameters**.

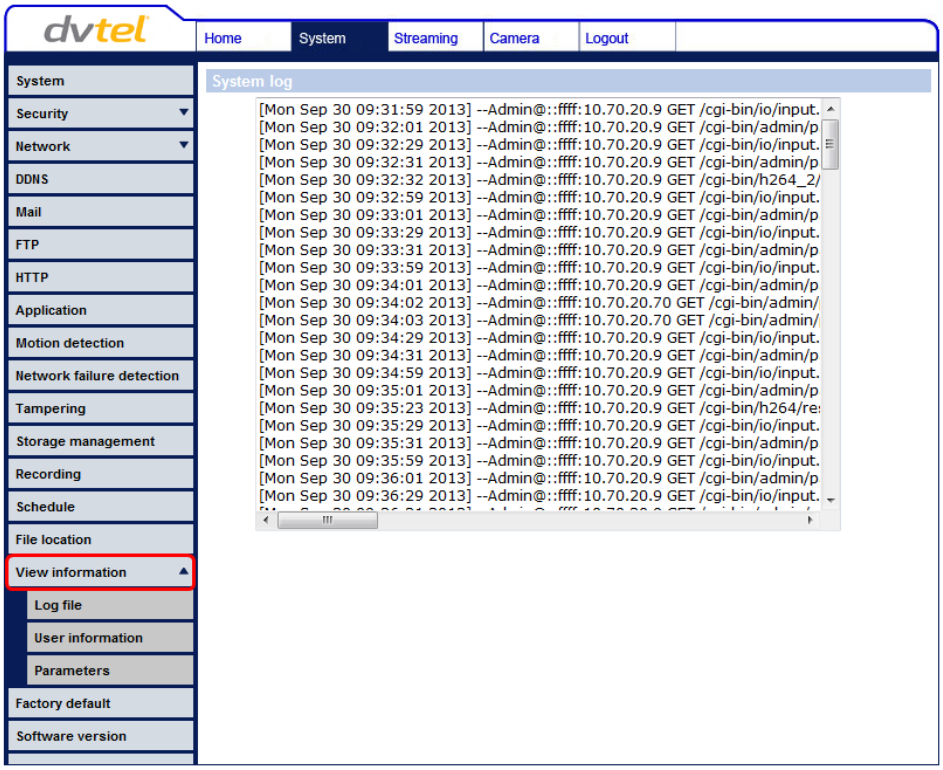

dvtel
Home
System
Streaming
Camera
Logout
System
Security
Network
DDNS
Mail
FTP
HTTP
Application
Motion detection
Network failure detection
Tampering
Storage management
Recording
Schedule
File location
View information
Log file
User information
Parameters
Factory default
Software version
System log
[Mon Sep 30 09:31:59 2013] --Admin@::ffff:10.70.20.9 GET /cgi-bin/io/input.
[Mon Sep 30 09:32:01 2013] --Admin@::ffff:10.70.20.9 GET /cgi-bin/admin/p
[Mon Sep 30 09:32:29 2013] --Admin@::ffff:10.70.20.9 GET /cgi-bin/io/input.
[Mon Sep 30 09:32:31 2013] --Admin@::ffff:10.70.20.9 GET /cgi-bin/admin/p
[Mon Sep 30 09:32:32 2013] --Admin@::ffff:10.70.20.9 GET /cgi-bin/h264_2/
[Mon Sep 30 09:32:59 2013] --Admin@::ffff:10.70.20.9 GET /cgi-bin/io/input.
[Mon Sep 30 09:33:01 2013] --Admin@::ffff:10.70.20.9 GET /cgi-bin/admin/p
[Mon Sep 30 09:33:29 2013] --Admin@::ffff:10.70.20.9 GET /cgi-bin/io/input.
[Mon Sep 30 09:33:31 2013] --Admin@::ffff:10.70.20.9 GET /cgi-bin/admin/p
[Mon Sep 30 09:33:59 2013] --Admin@::ffff:10.70.20.9 GET /cgi-bin/io/input.
[Mon Sep 30 09:34:01 2013] --Admin@::ffff:10.70.20.9 GET /cgi-bin/admin/p
[Mon Sep 30 09:34:02 2013] --Admin@::ffff:10.70.20.70 GET /cgi-bin/admin/
[Mon Sep 30 09:34:03 2013] --Admin@::ffff:10.70.20.70 GET /cgi-bin/admin/
[Mon Sep 30 09:34:29 2013] --Admin@::ffff:10.70.20.9 GET /cgi-bin/io/input.
[Mon Sep 30 09:34:31 2013] --Admin@::ffff:10.70.20.9 GET /cgi-bin/admin/p
[Mon Sep 30 09:34:59 2013] --Admin@::ffff:10.70.20.9 GET /cgi-bin/io/input.
[Mon Sep 30 09:35:01 2013] --Admin@::ffff:10.70.20.9 GET /cgi-bin/admin/p
[Mon Sep 30 09:35:23 2013] --Admin@::ffff:10.70.20.9 GET /cgi-bin/h264/re
[Mon Sep 30 09:35:29 2013] --Admin@::ffff:10.70.20.9 GET /cgi-bin/io/input.
[Mon Sep 30 09:35:31 2013] --Admin@::ffff:10.70.20.9 GET /cgi-bin/admin/p
[Mon Sep 30 09:35:59 2013] --Admin@::ffff:10.70.20.9 GET /cgi-bin/io/input.
[Mon Sep 30 09:36:01 2013] --Admin@::ffff:10.70.20.9 GET /cgi-bin/admin/p
[Mon Sep 30 09:36:29 2013] --Admin@::ffff:10.70.20.9 GET /cgi-bin/io/input.

Figure 67: System Log Screen

Related Links

- Log File
- User Information
- Parameters

7.3.16.1 Log File

Click **Log file** to view the system log file. The content of the file provides information about connections after system boot-up. See Figure 67: System Log Screen.

7.3.16.2 User Information

The Administrator can view each user's login information and privileges in the **User information** screen shown below.

View User Login Information

Click **get user information** to see each user's details. For example: *Admin: 1234*. This indicates that the user's login username is *Admin* and the password is *1234*.

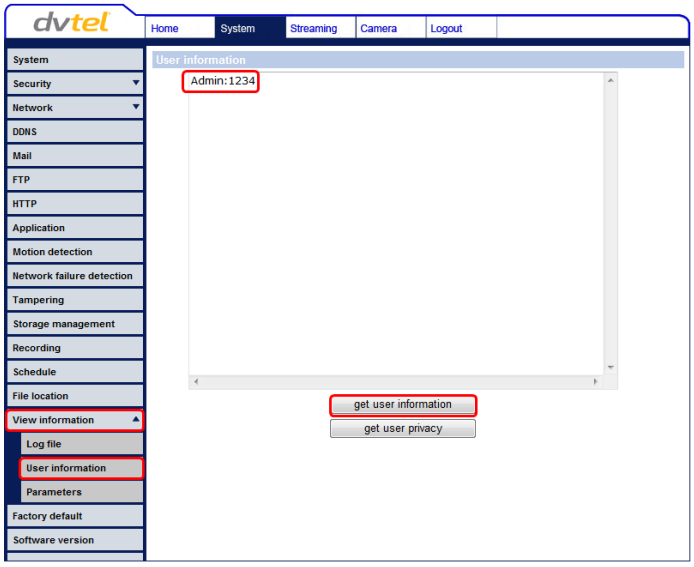


Figure 68: User Information Screen

View User Privilege

Click **get user privacy** to view each user's privileges.

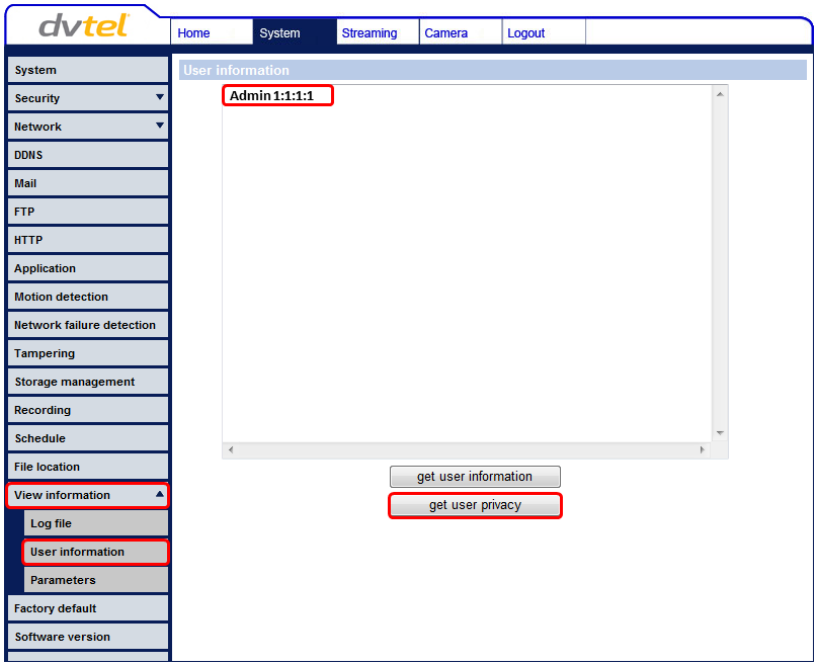
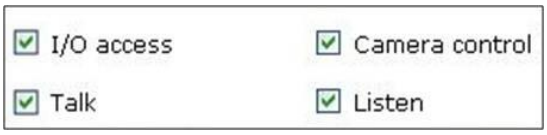


Figure 69: User Information – Privileges Screen

In the screen above, the user *Admin* is granted privileges of I/O access, Camera control, Talk and Listen.



Note:
The example above shows the maximum privileges that can be granted. It is however, dependent on the specific user security level.

7.3.16.3 Parameters

The **Parameter** screen enables viewing all of the system's parameter settings.

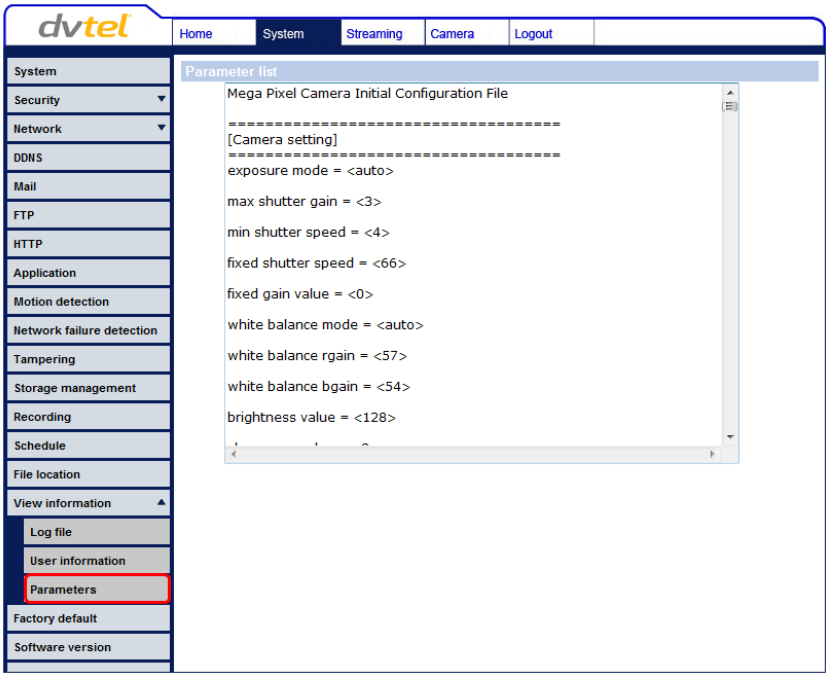


Figure 70: Parameter List Screen

Note:
Slide the sidebar located on the right of the screen to view the entire list of parameters.

7.3.17 Factory Default

The **Factory default** page is shown below. Follow the instructions to reset the camera to factory default settings if needed.

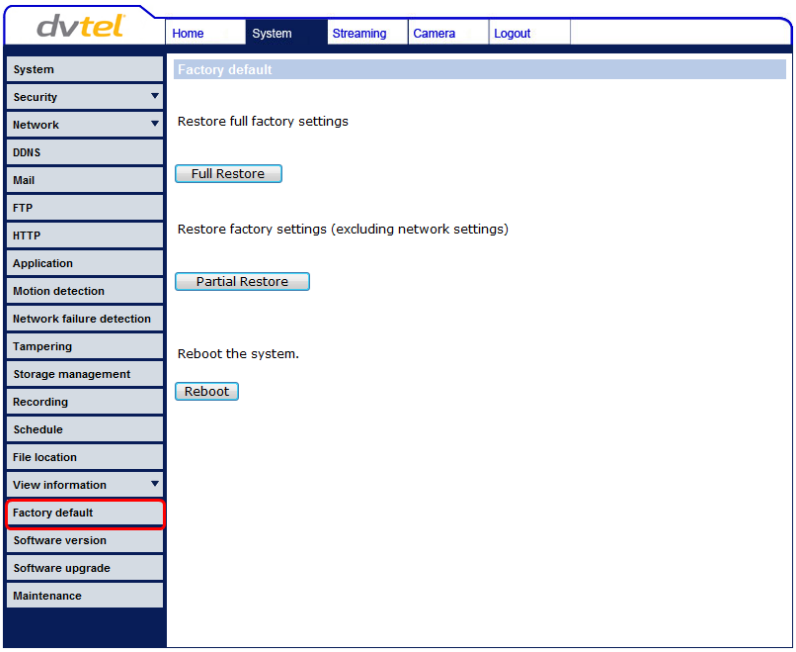


Figure 71: Factory Default Screen

Full Restore

Click **Full Restore** to restore the factory default settings. The system restarts in 30 seconds.

Note:
The IP address and all other settings will be restored to factory default settings.

Partial Restore

Click **Partial Restore** to restore the factory default settings, but save the network settings. The system restarts in 30 seconds.

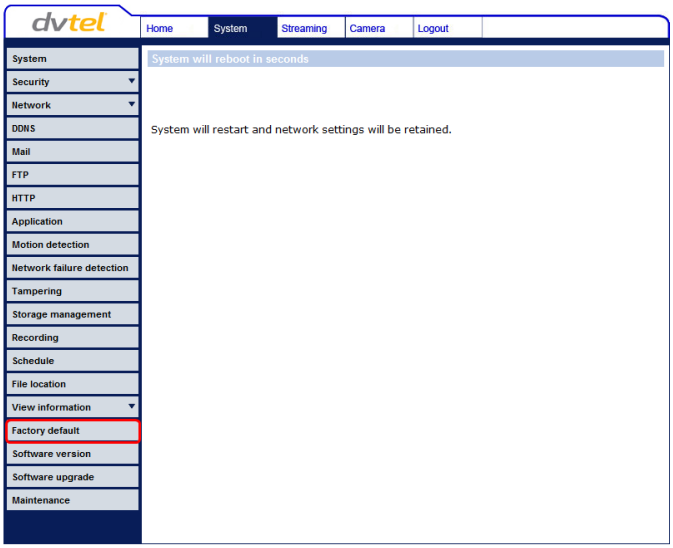


Figure 72: Partial Restore Screen

Reboot

Clicking **Reboot** restarts the system without changing current settings.

7.3.18 Software Version

The current version of software is displayed in the **Software version** screen.

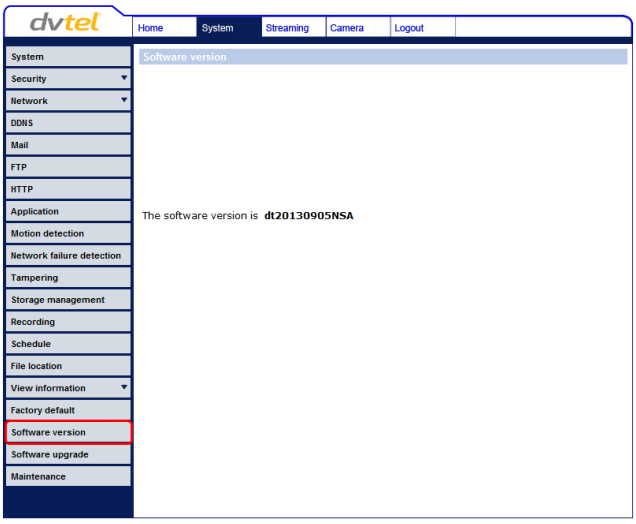


Figure 73: Software Version Screen

7.3.19 Software Upgrade

The **Upgrade** screen is shown below.

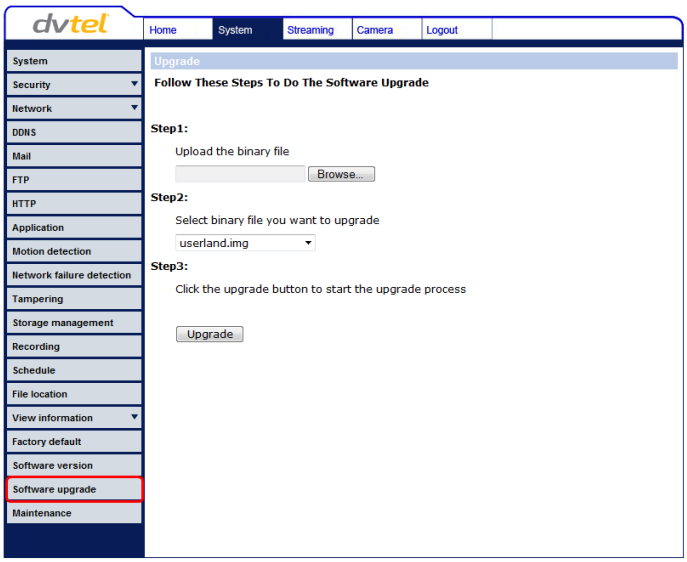


Figure 74: Upgrade Screen

Note:
Make sure that the software upgrade file is available before performing a software upgrade.

To upgrade the firmware:

1. In the *Step 1* text box, click **Browse** and select the binary file to be uploaded, for example, *uImage+userland.img*.

> **Note:**
> Do not change the upgrade file name or the system will fail to find the file.

2. From the drop-down menu of binary files in Step 2, select the file to upgrade. In the above example uImage+userland.img is selected.
3. Click Upgrade. The system verifies that the upgrade file exists and begins to upload the file. The upgrade status bar is displayed on the page. When the upgrade process is completed, the **Home** page is displayed.

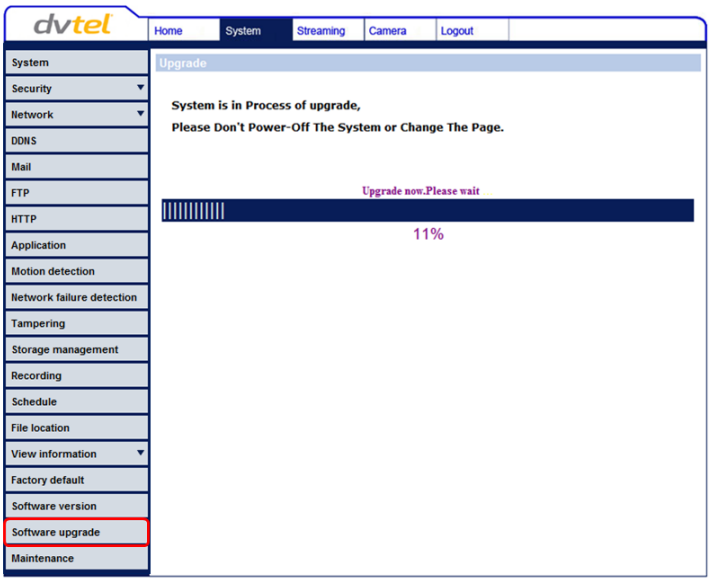


Figure 75: Software Upgrade – In Process

4. Close the video browser.
5. From the Windows Start menu, select Control Panel.
6. Select *Uninstall a Program.*
7. In the *Currently installed programs* list, select *DCViewer.*
8. Click **Uninstall** to delete the existing DCViewer.
9. Install the new DCViewer ActiveX plug-in.

> **Warning:**
> Do not unplug power while upgrading firmware.

7.3.20 Maintenance

You can export configuration files to a specified location and retrieve data by uploading an existing configuration file to the camera.

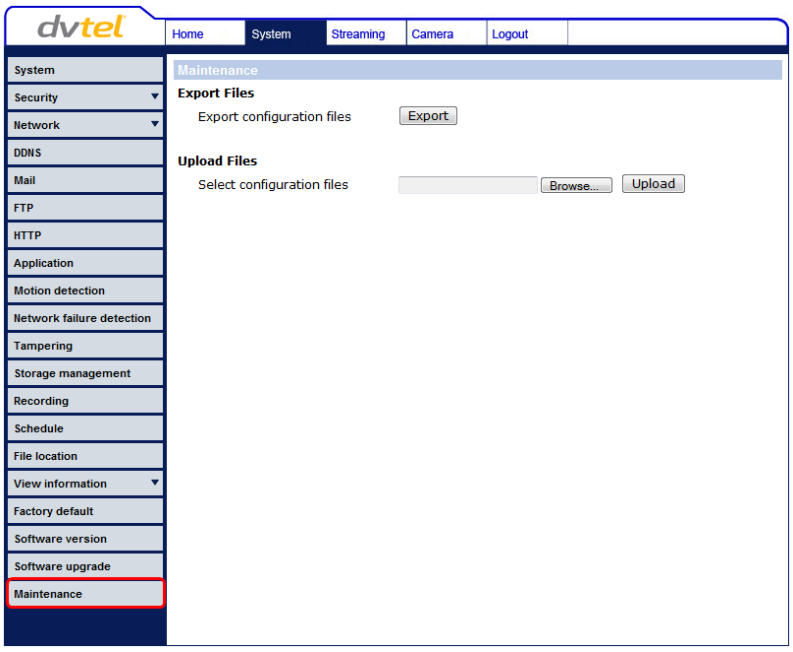


Figure 76: Maintenance Screen

Export

You can save system settings by exporting the configuration file (`.bin`) to a specified location for future use. Press **Export** and the popup window **File Download** appears as shown below.

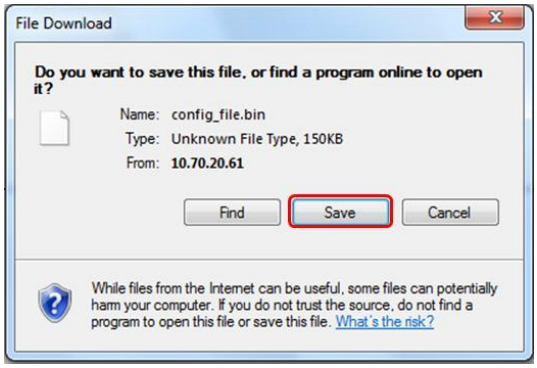

File Download
Do you want to save this file, or find a program online to open it?
Name: config_file.bin
Type: Unknown File Type, 150KB
From: 10.70.20.61
Find
Save
Cancel
While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not find a program to open this file or save this file. What's the risk?

Figure 77: File Download Screen

Click **Save** and specify a location to save the configuration file.

Warning:
Do not unplug power while changing file names.

Upload

To copy an existing configuration file to the camera, click **Browse** to select the configuration file, and then press **Upload** to upload the file.

Warning:
Do not unplug power while changing file names.

7.4 Video and Audio Streaming Settings

Select the **Streaming** tab in the navigation bar at the top of the page to display the configurable video and audio selections in the sidebar. From the Streaming sidebar, the Administrator can configure specific video resolution, video compression mode, video protocol, audio transmission mode, etc. Further details of these settings are specified in the following sections.

The following video resolutions are supported:

- H.264 + H.264
- MJPEG + H.264
- MJPEG only
- H.264 only

> **Note:**
> MJPEG is not supported by Latitude.

Related Links

- Video Format
- Video Frame Rate
- Video Compression
- Video Mask
- Video OCX Protocol
- Audio

7.4.1 Video Format

From the **Video Format** screen, you can configure the following settings:

- CM-3211 NTSC Video Resolution Settings
- CM-3211 PAL Video Resolution Settings
- CM-4221 NTSC Video Resolution Settings
- CM-4221 PAL Video Resolution Settings
- Text Overlay Settings
- Video Rotate Type
- GOV Settings
- H.264 Profile

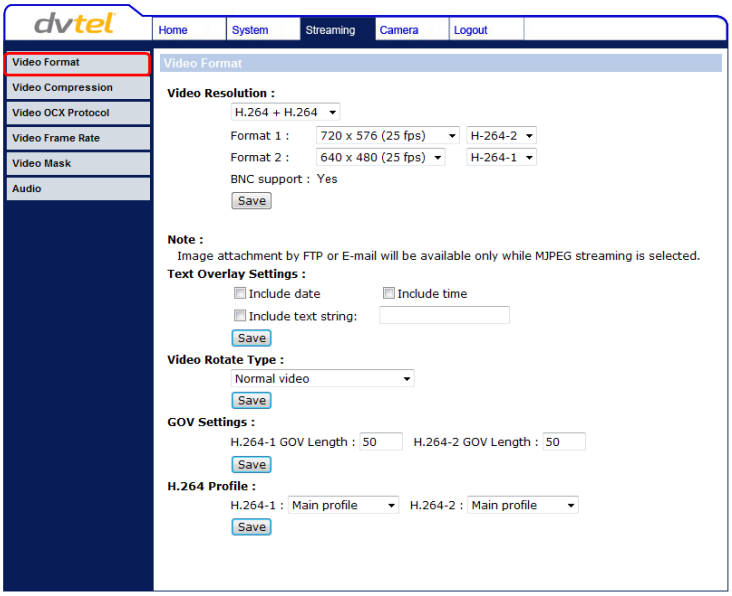


Figure 78: Video Format Screen

7.4.1.1 CM-3211 NTSC Video Resolution Settings

The following tables are video resolution settings for an NTSC TV system.

MJPEG + H.264 Video Resolution (NTSC):

H.264	MJPEG	BNC Support
1280 x 1024 (30fps)	1280 x 1024 (15fps)	√
	1280 x 720 (15fps)	-
	1024 x 768 (15fps)	-
	800 x 600 (30fps)	-
	720 x 480 (30fps)	√
	640 x 480 (30fps)	√
	352 x 240 (30fps)	√
1280 x 720 (30fps)	1280 x 720 (30fps)	√
	1024 x 768 (30fps)	-
	800 x 600 (30fps)	-
	720 x 480 (30fps)	√
	640 x 480 (30fps)	√
	352 x 240 (30fps)	√
1024 x 768 (30fps)	1024 x 768 (30fps)	√
	800 x 600 (30fps)	-
	720 x 480 (30fps)	√
	640 x 480 (30fps)	√
	352 x 240 (30fps)	√
800 x 600 (30fps)	800 x 600 (30fps)	√
	720 x 480 (30fps)	√
	640 x 480 (30fps)	√
	352 x 240 (30fps)	√
720 x 480 (30fps)	720 x 480 (30fps)	√
	640 x 480 (30fps)	√
	352 x 240 (30fps)	√
640 x 480 (30fps)	640 x 480 (30fps)	√
	352 x 240 (30fps)	√
352 x 240 (30fps)	352 x 240 (30fps)	-

Note:
MJPEG is not supported by Latitude.

H.264 + H.264 Video Resolution (NTSC):

H.264-1	H.264-2	BNC Support
1280 x 1024 (30fps)	1280 x 1024 (15fps)	√
	1280 x 720 (15fps)	-
	1024 x 768 (15fps)	-
	800 x 600 (30fps)	-
	720 x 480 (30fps)	√
	640 x 480 (30fps)	√
	352 x 240 (30fps)	√
1280 x 720 (30fps)	1280 x 720 (30fps)	√
	1024 x 768 (30fps)	-
	800 x 600 (30fps)	-
	720 x 480 (30fps)	√
	640 x 480 (30fps)	√
	352 x 240 (30fps)	√
1024 x 768 (30fps)	1024 x 768 (30fps)	√
	800 x 600 (30fps)	-
	720 x 480 (30fps)	√
	640 x 480 (30fps)	√
	352 x 240 (30fps)	√
800 x 600 (30fps)	800 x 600 (30fps)	√
	720 x 480 (30fps)	√
	640 x 480 (30fps)	√
	352 x 240 (30fps)	√
720 x 480 (30fps)	720 x 480 (30fps)	√
	640 x 480 (30fps)	√
	352 x 240 (30fps)	√
640 x 480 (30fps)	640 x 480 (30fps)	√
	352 x 240 (30fps)	√
352 x 240 (30fps)	352 x 240 (30fps)	-

MJPEG Only Video Resolution (NTSC):

MJPEG	BNC Support
1280 x 1024 (30fps)	√
1280 x 720 (30fps)	√
1024 x 768 (30fps)	√
800 x 600 (30fps)	√
720 x 480 (30fps)	√
640 x 480 (30fps)	√
352 x 240 (30fps)	-

Note:
MJPEG is not supported by Latitude.

H.264 Only Video Resolution (NTSC):

H.264	BNC Support
1280 x 1024 (30fps)	√
1280 x 720 (30fps)	√
1024 x 768 (30fps)	√
800 x 600 (30fps)	√
720 x 480 (30fps)	√
640 x 480 (30fps)	√
352 x 240 (30fps)	-

7.4.1.2 CM-3211 PAL Video Resolution Settings

The following tables are video resolution settings for a PAL system.

MJPEG + H.264 Video Resolution (PAL):

H.264	MJPEG	BNC Support
1280 x 1024 (25fps)	1280 x 1024 (13fps)	√
	1280 x 720 (13fps)	-
	1024 x 768 (13fps)	-
	800 x 600 (25fps)	-
	720 x 576 (25fps)	√
	640 x 480 (25fps)	√
	352 x 288 (25fps)	√
1280 x 720 (25fps)	1280 x 720 (25fps)	√
	1024 x 768 (25fps)	-
	800 x 600 (25fps)	-
	720 x 576 (25fps)	√
	640 x 480 (25fps)	√
	352 x 288 (25fps)	√
1024 x 768 (25fps)	1024 x 768 (25fps)	√
	800 x 600 (25fps)	-
	720 x 576 (25fps)	√
	640 x 480 (25fps)	√
	352 x 288 (25fps)	√
800 x 600 (25fps)	800 x 600 (25fps)	√
	720 x 576 (25fps)	√
	640 x 480 (25fps)	√
	352 x 288 (25fps)	√
720 x 576 (25fps)	720 x 576 (25fps)	√
	640 x 480 (25fps)	√
	352 x 288 (25fps)	√
640 x 480 (25fps)	640 x 480 (25fps)	√
	352 x 288 (25fps)	√
352 x 288 (25fps)	352 x 288 (25fps)	-

Note:
MJPEG is not supported by Latitude.

H.264 + H.264 Video Resolution (PAL):

H.264-1	H.264-2	BNC Support
1280 x 1024 (25fps)	1280 x 1024 (13fps)	√
	1280 x 720 (13fps)	-
	1024 x 768 (13fps)	-
	800 x 600 (25fps)	-
	720 x 576 (25fps)	√
	640 x 480 (25fps)	√
	352 x 288 (25fps)	√
1280 x 720 (25fps)	1280 x 720 (25fps)	√
	1024 x 768 (25fps)	-
	800 x 600 (25fps)	-
	720 x 576 (25fps)	√
	640 x 480 (25fps)	√
	352 x 288 (25fps)	√
1024 x 768 (25fps)	1024 x 768 (25fps)	√
	800 x 600 (25fps)	-
	720 x 576 (25fps)	√
	640 x 480 (25fps)	√
	352 x 288 (25fps)	√
800 x 600 (25fps)	800 x 600 (25fps)	√
	720 x 576 (25fps)	√
	640 x 480 (25fps)	√
	352 x 288 (25fps)	√
720 x 576 (25fps)	720 x 576 (25fps)	√
	640 x 480 (25fps)	√
	352 x 288 (25fps)	√
640 x 480 (25fps)	640 x 480 (25fps)	√
	352 x 288 (25fps)	√
352 x 288 (25fps)	352 x 288 (25fps)	-

MJPEG Only Video Resolution (PAL):

MJPEG	BNC Support
1280 x 720 (25fps)	√
1024 x 768 (25fps)	√
800 x 600 (25fps)	√
720 x 576 (25fps)	√
640 x 480 (25fps)	√
352 x 288 (25fps)	-

Note:
MJPEG is not supported by Latitude.

H.264 Only Video Resolution (PAL):

H.264	BNC Support
1280 x 1024 (25fps)	√
1280 x 720 (25fps)	√
1024 x 768 (25fps)	√
800 x 600 (25fps)	√
720 x 576 (25fps)	√
640 x 480 (25fps)	√
352 x 288 (25fps)	-

7.4.1.3 CM-4221 NTSC Video Resolution Settings

The following tables are video resolution settings for an NTSC TV system.

MJPEG + H.264 Video Resolution (NTSC):

H.264	MJPEG	BNC Support
1920 x 1080 (30 fps)	720 x 480 (30fps)	√
	640 x 480 (30fps)	√
	352 x 240 (30fps)	√
1920 x 1080 (15 fps)	1920 x 1080 (15 fps)	√
	1280 x 1024 (30fps)	-
	1280 x 720 (30fps)	-
	1024 x 768 (30fps)	-
	800 x 600 (30fps)	-
1280 x 1024 (30fps)	1280 x 1024 (15fps)	√
	1280 x 720 (30fps)	-
	1024 x 768 (30fps)	-
	800 x 600 (30fps)	-
	720 x 480 (30fps)	√
	640 x 480 (30fps)	√
	352 x 240 (30fps)	√
1280 x 720 (30fps)	1280 x 720 (30fps)	√
	1024 x 768 (30fps)	-
	800 x 600 (30fps)	-
	720 x 480 (30fps)	√
	640 x 480 (30fps)	√
	352 x 240 (30fps)	√
1024 x 768 (30fps)	1024 x 768 (30fps)	√
	800 x 600 (30fps)	-
	720 x 480 (30fps)	√
	640 x 480 (30fps)	√
	352 x 240 (30fps)	√
800 x 600 (30fps)	800 x 600 (30fps)	√
	720 x 480 (30fps)	√
	640 x 480 (30fps)	√
	352 x 240 (30fps)	√
720 x 480 (30fps)	720 x 480 (30fps)	√
	640 x 480 (30fps)	√
	352 x 240 (30fps)	√
640 x 480 (30fps)	640 x 480 (30fps)	√
	352 x 240 (30fps)	√
352 x 240 (30fps)	352 x 240 (30fps)	-

Note:
MJPEG is not supported by Latitude.

H.264 + H.264 Video Resolution (NTSC):

H.264-1	H.264-2	BNC Support
1920 x 1080 (30 fps)	720 x 480 (30fps)	√
	640 x 480 (30fps)	√
	352 x 240 (30fps)	√
1920 x 1080 (15 fps)	1920 x 1080 (15 fps)	√
	1280 x 1024 (30fps)	-
	1280 x 720 (30fps)	-
	1024 x 768 (30fps)	-
	800 x 600 (30fps)	-
1280 x 1024 (30fps)	1280 x 1024 (15fps)	√
	1280 x 720 (30fps)	-
	1024 x 768 (15fps)	-
	800 x 600 (30fps)	-
	720 x 480 (30fps)	√
	640 x 480 (30fps)	√
	352 x 240 (30fps)	√
1280 x 720 (30fps)	1280 x 720 (30fps)	√
	1024 x 768 (30fps)	-
	800 x 600 (30fps)	-
	720 x 480 (30fps)	√
	640 x 480 (30fps)	√
	352 x 240 (30fps)	√
1024 x 768 (30fps)	1024 x 768 (30fps)	√
	800 x 600 (30fps)	-
	720 x 480 (30fps)	√
	640 x 480 (30fps)	√
	352 x 240 (30fps)	√
800 x 600 (30fps)	800 x 600 (30fps)	√
	720 x 480 (30fps)	√
	640 x 480 (30fps)	√
	352 x 240 (30fps)	√
720 x 480 (30fps)	720 x 480 (30fps)	√
	640 x 480 (30fps)	√
	352 x 240 (30fps)	√
640 x 480 (30fps)	640 x 480 (30fps)	√
	352 x 240 (30fps)	√
352 x 240 (30fps)	352 x 240 (30fps)	-

MJPEG-Only Video Resolution (NTSC):

MJPEG	BNC Support
1920 x 1080 (30fps)	√
1280 x 1024 (30fps)	√
1280 x 720 (30fps)	√
1024 x 768 (30fps)	√
800 x 600 (30fps)	√
720 x 576 (30fps)	√
640 x 480 (30fps)	√
352 x 288 (30fps)	-

Note:
MJPEG is not supported by Latitude.

H.264-Only Video Resolution (NTSC):

H.264	BNC Support
1920 x 1080 (30fps) Low latency	-
1920 x 1080 (30fps)	√
1280 x 1024 (30fps)	√
1280 x 720 (30fps)	√
1024 x 768 (30fps)	√
800 x 600 (30fps)	√
720 x 480 (30fps)	√
640 x 480 (30fps)	√
352 x 240 (30fps)	-

7.4.1.4 CM-4221 PAL Video Resolution Settings

The following tables are video resolution settings for a PAL system.

MJPEG + H.264 Video Resolution (PAL):

H.264	MJPEG	BNC Support
1920 x 1080 (25fps)	1920 x 1080 (25fps)	√
	720 x 576 (25fps)	√
	640 x 480 (25fps)	√
	352 x 288 (25fps)	√
1920 x 1080 (13fps)	1920 x 1080 (13fps)	√
	1280 x 1024 (25fps)	√
	1280 x 720 (25fps)	√
	1024 x 768 (25fps)	√
	800 x 600 (25fps)	-
1280 x 1024 (25fps)	1280 x 1024 (13fps)	√
	1280 x 720 (26fps)	-
	1024 x 768 (25fps)	-
	800 x 600 (25fps)	-
	720 x 576 (25fps)	√
	640 x 480 (25fps)	√
	352 x 288 (25fps)	√
1280 x 720 (25fps)	1280 x 720 (25fps)	√
	1024 x 768 (25fps)	-
	800 x 600 (25fps)	√
	720 x 576 (25fps)	√
	640 x 480 (25fps)	√
	352 x 288 (25fps)	√
1024 x 768 (25fps)	1024 x 768 (25fps)	-
	800 x 600 (25fps)	-
	720 x 576 (25fps)	√
	640 x 480 (25fps)	√
	352 x 288 (25fps)	√
800 x 600 (25fps)	800 x 600 (25fps)	√
	720 x 576 (25fps)	-
	640 x 480 (25fps)	√
	352 x 288 (25fps)	√
720 x 576 (25fps)	720 x 576 (25fps)	√
	640 x 480 (25fps)	√
	352 x 240 (25fps)	√
640 x 480 (25fps)	640 x 480 (25fps)	√
	352 x 288 (25fps)	√
352 x 288 (25fps)	352 x 288 (25fps)	-

Note:
MJPEG is not supported by Latitude.

H.264 + H.264 Video Resolution (PAL):

H.264-1	H.264-2	BNC Support
1920 x 1080 (25fps)	1920 x 1080 (25fps)	√
	720 x 576 (25fps)	√
	640 x 480 (25fps)	√
	352 x 288 (25fps)	√
1920 x 1080 (13fps)	1920 x 1080 (13fps)	√
	1280 x 1024 (25fps)	√
	1280 x 720 (13fps)	√
	1024 x 768 (13fps)	√
	800 x 600 (25fps)	-
1280 x 1024 (25fps)	1280 x 1024 (13fps)	√
	1280 x 720 (25fps)	-
	1024 x 768 (25fps)	-
	800 x 600 (25fps)	-
	720 x 576 (25fps)	√
	640 x 480 (25fps)	√
	352 x 288 (25fps)	√
1280 x 720 (25fps)	1280 x 720 (25fps)	√
	1024 x 768 (25fps)	-
	800 x 600 (25fps)	√
	720 x 576 (25fps)	√
	640 x 480 (25fps)	√
	352 x 288 (25fps)	√
1024 x 768 (25fps)	1024 x 768 (25fps)	-
	800 x 600 (25fps)	-
	720 x 576 (25fps)	√
	640 x 480 (25fps)	√
	352 x 288 (25fps)	√
800 x 600 (25fps)	800 x 600 (25fps)	√
	720 x 576 (25fps)	-
	640 x 480 (25fps)	√
	352 x 288 (25fps)	√
720 x 576 (25fps)	720 x 576 (25fps)	√
	640 x 480 (25fps)	√
	352 x 288 (25fps)	√
640 x 480 (25fps)	640 x 480 (25fps)	√
	352 x 288 (25fps)	√
352 x 288 (25fps)	352 x 288 (25fps)	-

MJPEG-Only Video Resolution (PAL):

MJPEG	BNC Support
1980 x 1080 (25fps)	√
1280 x 1024 (25fps)	√
1280 x 720 (25fps)	√
1024 x 768 (25fps)	√
800 x 600 (25fps)	√
720 x 576 (25fps)	√
640 x 480 (25fps)	√
352 x 288 (25fps)	-

Note:
MJPEG is not supported by Latitude.

H.264-Only Video Resolution (PAL):

H.264	BNC Support
1920 x 1080 (25fps) - Low latency	√
1920 x 1080 (25fps)	√
1280 x 1024 (25fps)	√
1280 x 720 (25fps)	√
1024 x 768 (25fps)	√
800 x 600 (25fps)	√
720 x 576 (25fps)	√
640 x 480 (25fps)	√
352 x 288 (25fps)	√

7.4.1.5 Text Overlay Settings

You can select the options to display data including date/time/text on the live video pane. The maximum length of the string is 20 alphanumeric characters. Click **Save** to confirm the Text Overlay setting.

7.4.1.6 Video Rotate Type

You can change video display type if necessary. Selectable video rotate types include Normal video, Flip video, Mirror video, 90 degree clockwise, 180 degree rotate, and 90 degree counterclockwise. Differences among these types are illustrated below. The following drop-down menu appears when selecting this option.

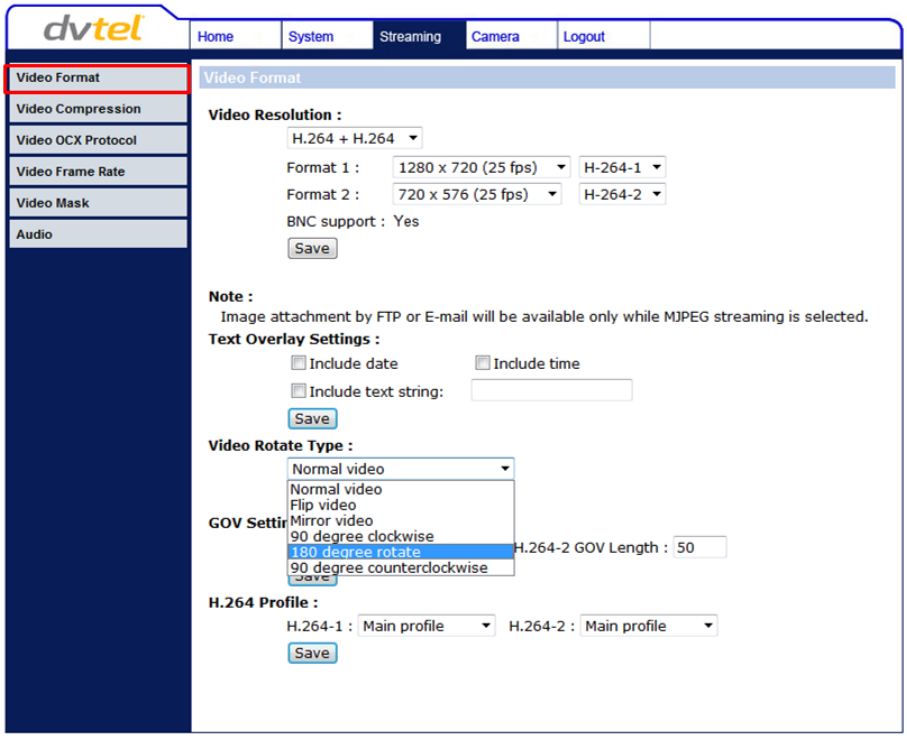


Figure 79: Video Rotate Type Screen

Suppose the displayed image of the camera is shown as follows.

Figure 80: View-1 (Source)

To rotate the image vertically, for example, select *Flip video*. The displayed image is reversed as shown below.

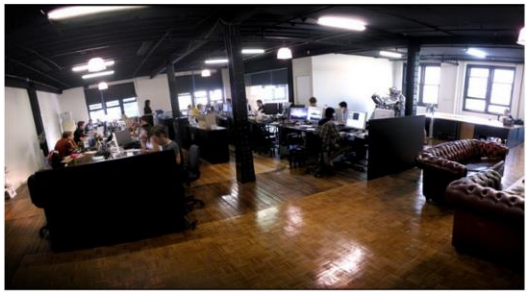


Figure 81: View-2 Image Rotated Vertically (Reversed)

Following are descriptions of different video rotate types.

- *Normal video* – The image appears as it is viewed.
- *Flip video* – The image is reversed along its horizontal axis.
- *Mirror video* – The image is reversed along its vertical axis.
- *90 degree clockwise* – The image rotates 90° clockwise (to the right).
- *180 degree rotate* – The image rotates 180° counter-clockwise (to the left).
- *90 degree counterclockwise* – The image rotates 90° counter-clockwise (to the left).

Click **Save** to confirm the setting.

7.4.1.7 GOV Settings

Users can set the GOV length to determine the frame structure (I-frames and P-frames) in a video stream for saving bandwidth. The setting range is from 2 to 64. A longer GOV means decreasing the frequency of I-frames. Click **Save** to confirm the GOV setting.

7.4.1.8 H.264 Profile

The H.264 standard defines 21 sets of capabilities. These are referred to as profiles and they target specific classes of applications. In the security industry, the most common are as follows:

- **Baseline Profile (BP)**
  Primarily for low-cost applications that require additional data loss robustness, *Baseline Profile* is used in some videoconferencing and mobile applications. This is the most common profile used in IP security cameras due to the low computational cost of processing the video using this profile

- **Main Profile (MP)**
  This profile provides improved picture quality at reduced bandwidths and storage costs and is becoming more common as the camera processors (DSPs) become more able to handle the processing load. *Main Profile* can save 10-30% over *Baseline*.
- **High Profile (HP)**
  High Profile is the primary profile for HD broadcast and Blu-ray HD disc media applications. It can save 10-30% of the storage cost over *Main Profile*. However, it may also increase video latency, depending on the stream structure. Quasar models default to the *Main Profile* to provide the best trade-off between storage size and video latency.

Click **Save** to confirm the settings.

7.4.2 Video Compression

From the **Video Compression** page, you can specify MJPEG/H.264 compression settings.

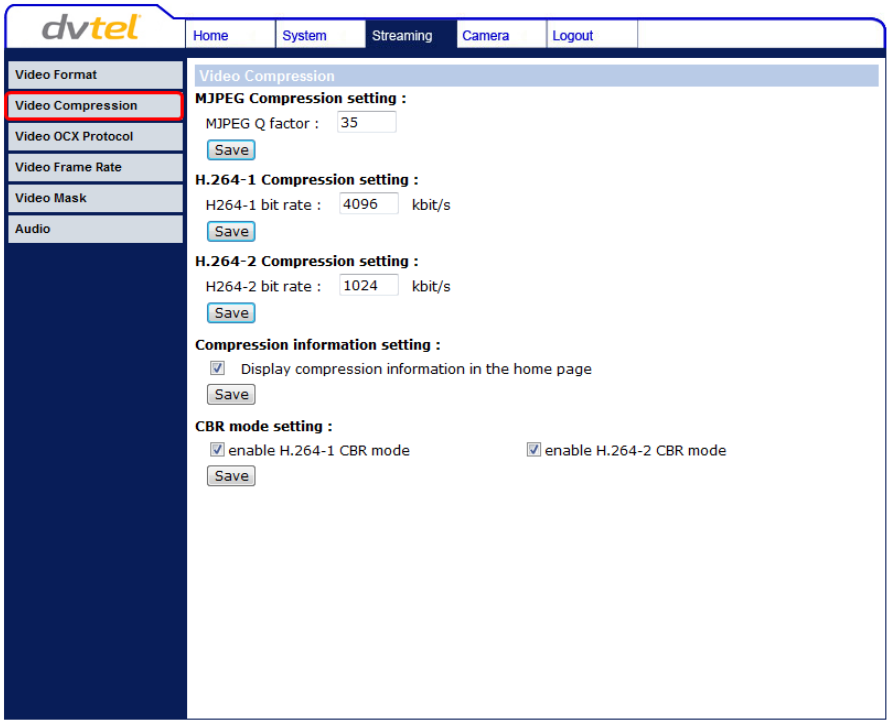


Figure 82: Video Compression Screen

MJPEG Compression Setting

A higher value implies higher bit rates and higher visual quality. The default setting of the MJPEG Q factor is 35. The setting range is from 1 to 70. Click **Save** to confirm the setting.

Note:
MJPEG is not supported by Latitude.

H.264-1/H.264-2 Compression Setting

The default setting of H.264-1/H.264-2 is 4096/1024 kbps. The setting range is from 64 to 8192 kbps. Click **Save** to confirm the setting.

Note:
The second stream is limited to 2048 kbps.

Compression Information Setting

Select the checkbox to display compression information on the **Home** page. Click **Save** to confirm the setting.

CBR Mode Setting

If available bandwidth is limited, CBR (Constant Bit Rate) mode can be selected. To operate the camera in Variable Bit Rate (VBR) mode, uncheck the CBR checkbox. Click **Save** to confirm the setting.

Note:
CBR mode affects image quality.

7.4.3 Video OCX Protocol

From the **Video OCX Protocol** page, you can select various protocols for streaming media over the network. In the case of multicast networking, select **Multicast mode**.

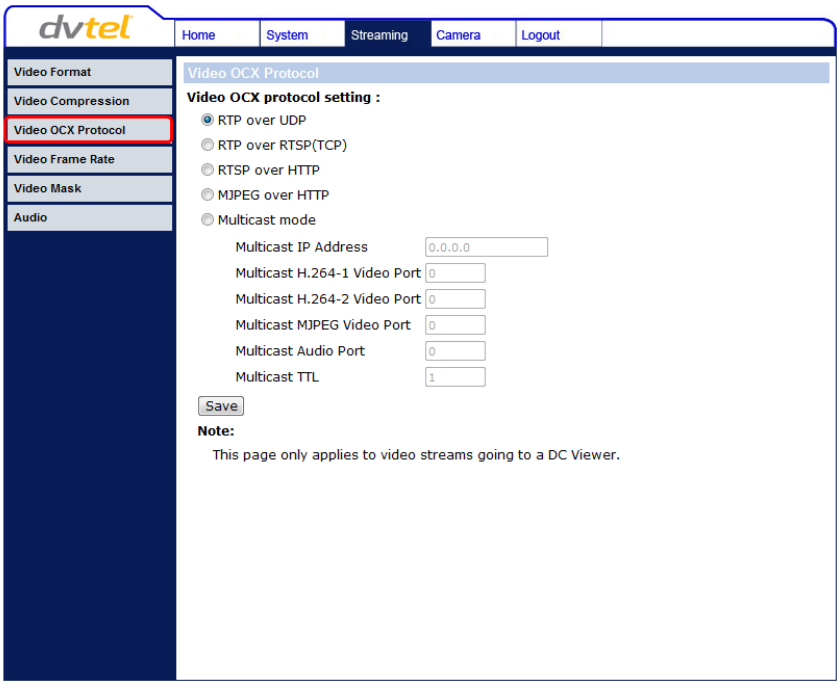


Figure 83: Video OCX Protocol Screen

Video OCX protocol setting options include:

- *RTP over UDP*
- *RTP over RTSP (TCP)*
- *RTSP over HTTP*
- *MJPEG over HTTP*
- *Multicast mode* – Enter in each field all required data, including *Multicast IP address, H.264-1 video port, H.264-2 video port, MJPEG video port, MJPEG audio port,* and *Multicast TTL*.

Note:
MJPEG is not supported by Latitude.

Click **Save** to confirm the settings.

7.4.4 Video Frame Rate

From the **Video Frame Rate** screen, you can specify the frames per second (fps) for each video compression format.

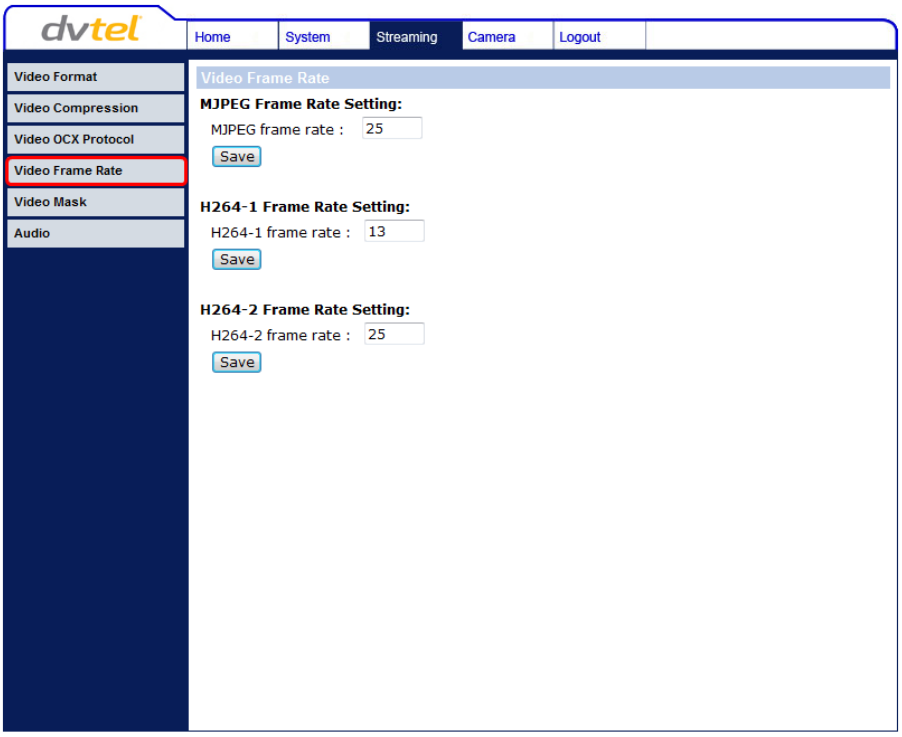


Figure 84: Video Frame Rate Screen

MJPEG/H.264-1/H.264-2 Frame Rate Setting

The default setting of the MJPEG Frame Rate is 30 fps in NTSC and 25 fps in PAL.

The setting range for the H-264-1 Frame Rate is from 1 to 30 in NTSC and 1 to 25 in PAL.

The setting range for the H-264-2 Frame Rate is from 1 to 30 in NTSC and 1 to 25 in PAL.

Click **Save** to confirm the settings.

Note:
MJPEG is not supported by Latitude.

Note:
A lower frame rate decreases video smoothness.

7.4.5 Video Mask

From the **Mask** screen, you may select up to five rectangular portions of the View Area to 'Mask.' Below is an illustration with the maximum five masks displayed in the View Area, the last (fifth) one selected being highlighted in red.

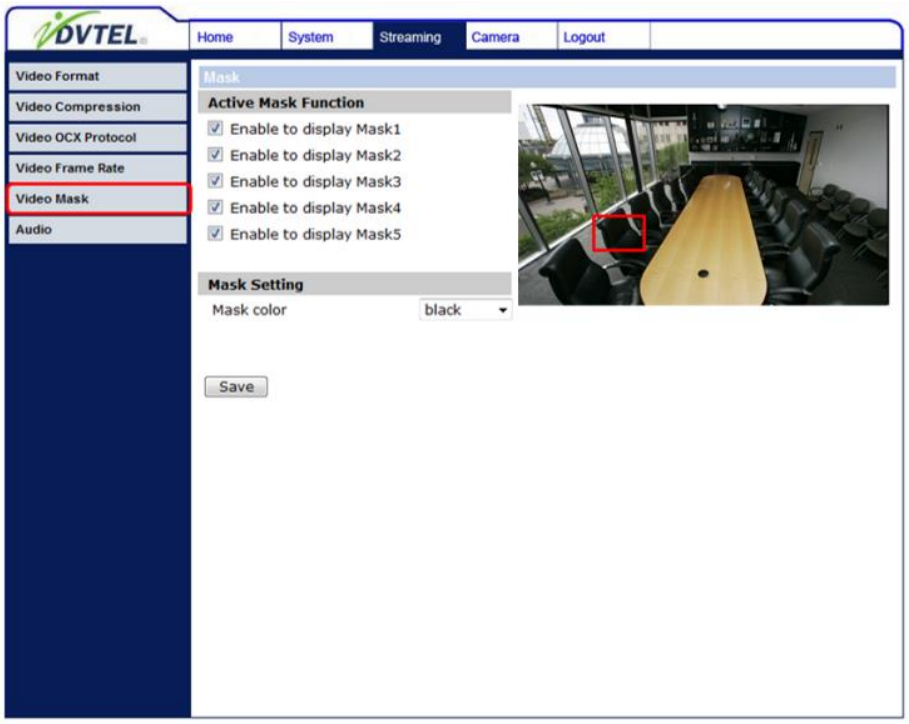


Figure 85: Mask Screen

Active Mask Function

When a Video [Privacy] Mask is turned on, the area within the mask or box is blocked out or obscured from view.

To enable a mask:

1. Check a Video Mask checkbox. A red frame is displayed in the Live Video pane on the right side.
2. Use the mouse to drag and drop, adjust the mask's size, and place it on the target zone.

> **Note:**
> It is suggested to set the Video Mask twice as large as the object it covers.

To disable a mask:

3. Uncheck the checkbox of the Video Mask meant to be deleted. The selected mask disappears from the Live Video pane.

Mask Setting

- Mask color – The selections of Mask color include red, black, white, yellow, green, blue, cyan, and magenta. Click **Save** to confirm the setting.

7.4.6 Audio

From the **Audio** screen you can select the Transmission Mode, Server Gain, Bit Rate, and enable or disable storage of the audio recording.

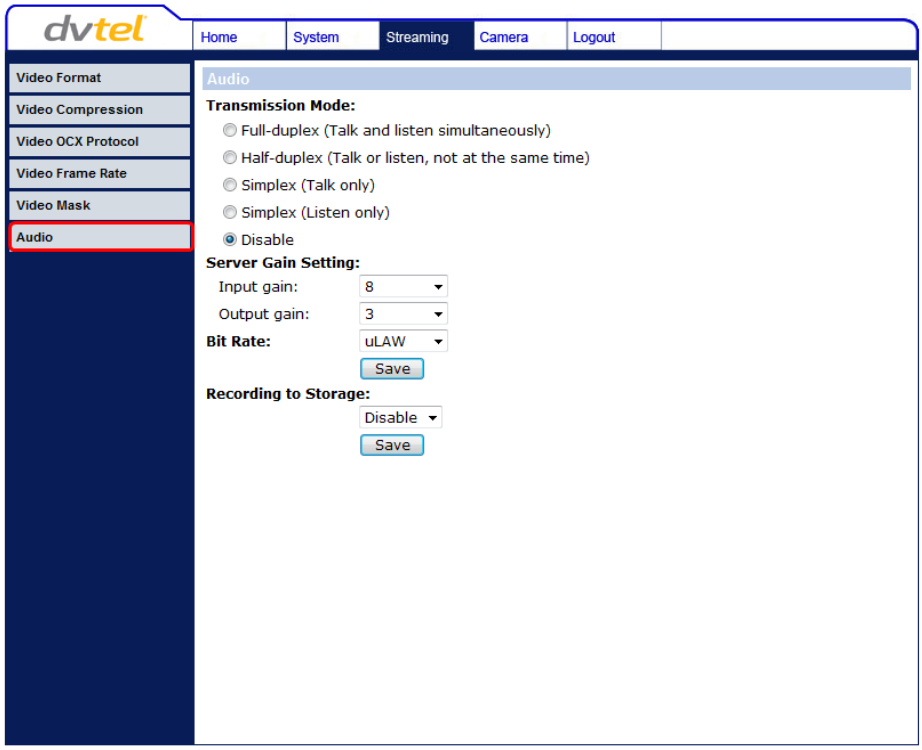


Figure 86: Audio Screen

Transmission Mode

- *Full-duplex (Talk and listen simultaneously)* – In the Full-duplex mode, the local and remote sites can communicate with each other simultaneously, i.e. both sites can speak and be heard at the same time.
- *Half-duplex (Talk or listen, not at the same time)* – In the Half-duplex mode, the local or remote site can only talk or listen to the other site at one time.
- *Simplex (Talk only)* – In the Talk only Simplex mode, the local/remote site can only talk to the other site.
- *Simplex (Listen only)* – In the Listen only Simplex mode, the local/remote site can only listen to the other site.
- *Disable* – Select this option to turn off the audio transmission function.

Server Gain Setting

Set the audio input/output gain levels for sound amplification. The audio gain values are adjustable from 1 to 6. The sound will be turned off if the audio gain is set to *Mute*.

Bit Rate

Selectable audio transmission bit rate include 16 kbps (G.726), 24 kbps (G.726), 32 kbps (G.726), 40 kbps (G.726), µLAW (G.711) and ALAW (G.711). Both µLAW and ALAW signify 64 kbps, but in different compression formats. A higher bit rate enables higher audio quality, but requires higher bandwidth.

Note:
Latitude does not support G.726 bit rates.

Click **Save** to confirm the settings.

Recording to Storage

This function enables recording of the audio on the SD card. The *Recording to Storage* function may be enabled or disabled in the **Audio** screen. The default setting is *Disabled.*

Note:
This function works only if the *Recording to Storage* option has been selected or if the *Schedule* option has been set.

Click **Save** to confirm the settings.

7.5 Camera-Related Settings

From the **Camera** tab, the administrator can adjust any of the camera settings, such as Exposure, White Balance, Picture Adjustment, Backlight, Digital Zoom, IR Function, WDR Function, Noise Reduction, and TV System.

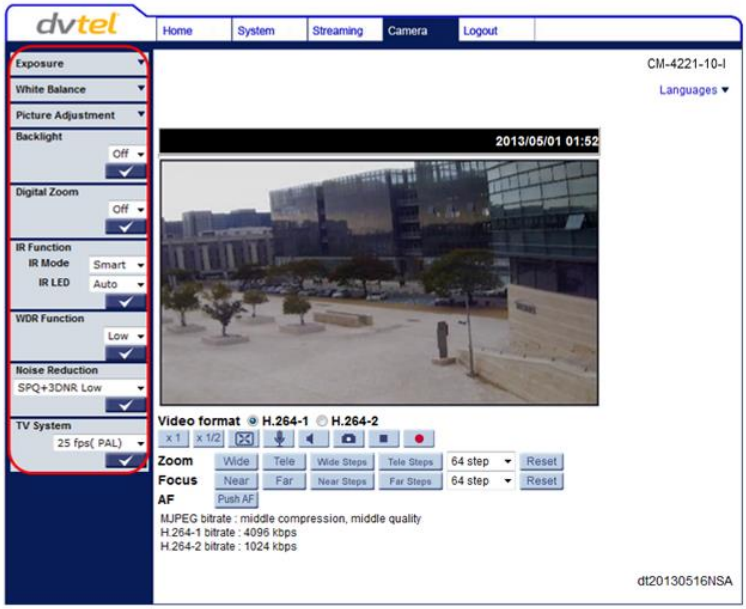


Figure 87: Camera Settings Screen

Related Links:

- Exposure
- White Balance
- Picture Adjustment
- Backlight
- Digital Zoom
- IR Function
- WDR Function
- Noise Reduction
- TV System

7.5.1 Exposure

The exposure is the amount of light received by the image sensor and is determined by the amount of exposure by the sensor (shutter speed), and other exposure parameters.

Administrators may either allow the camera to automatically select an exposure level using a programmed algorithm or choose the level themselves. Even in Auto Shutter, a Minimum Shutter Speed may be set from the drop-down menu to ensure a maximum level of exposure. In Manual Mode, the administrator can choose fixed shutter speeds from a drop-down menu. The smaller the number (the higher the shutter speed) that the administrator selects, the lower the exposure level and vice versa. Following is an illustration of the **Camera** menu.

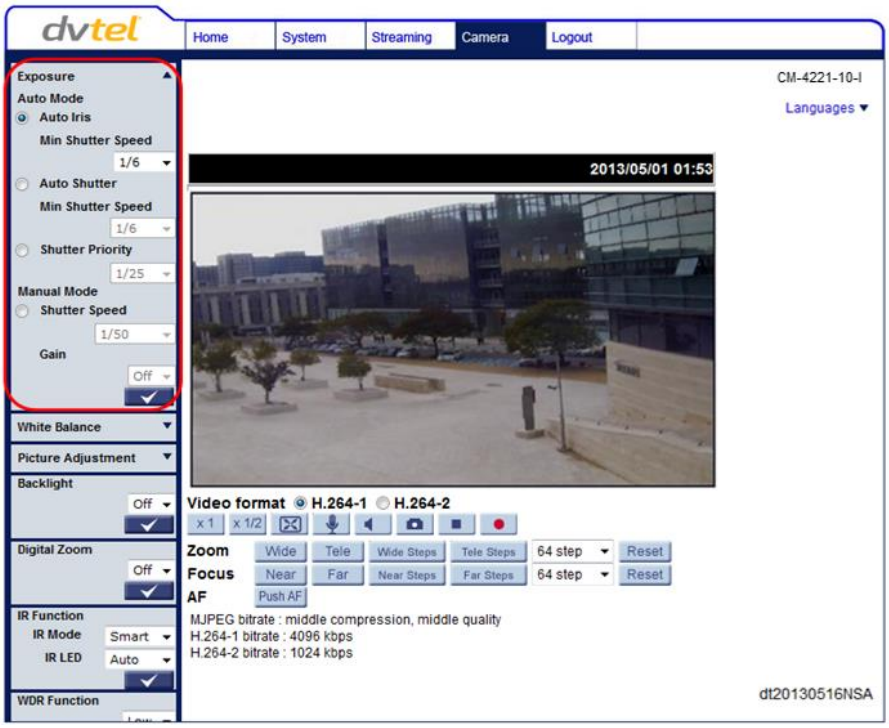


Figure 88: Camera Settings Screen – Exposure

There are two exposure modes: *Auto Mode* and *Manual Mode*.

Auto Mode

There are three settings within *Auto Mode:*

- *Auto Iris Min Shutter Speed* – When selecting this mode, the shutter is completely open and the exposure priority is given to the iris. Shutter speed and AGC circuit function automatically in cooperating with the iris to achieve a consistent exposure output.

  The shutter speed range is from 1 to 1/30 sec (NTSC) and 1/1.5 to 1/25 sec (PAL). See the table below showing all the options.

Auto Iris - Min Shutter Speed	
PAL	NTSC
1/25	1/30
1/12	1/15
1/6	1/8
1/3	1/4
1/1.5	1/2
	1

- *Auto Shutter Min Shutter Speed* – When selecting this mode, the camera's shutter speed works automatically to achieve a consistent video output level. Users can select a suitable shutter speed according to the environmental luminance.

  The shutter speed range is from 1 to 1/500 sec (NTSC) and 1/1.5 to 1/425 sec (PAL). See following table, which shows all the options.

Auto Shutter – Min Shutter speed	
PAL	NTSC
1/425	1/500
1/300	1/350
1/215	1/250
1/150	1/180
1/120	1/120
1/100	1/100
1/75	1/90
1/50	1/60
1/25	1/30
1/12	1/15
1/6	1/8
1/3	1/4
1/1.5	1/2
	1

- *Shutter Priority* – When selecting this mode, a fixed exposure is set, while other parameters can change. The shutter speed range is from 1 to 1/500 sec (NTSC) and 1/1.5 to 1/425 sec (PAL). See table below showing all the options.

Shutter Speed Priority	
PAL	NTSC
1/425	1/500
1/300	1/350
1/215	1/250
1/150	1/180
1/120	1/120
1/100	1/100
1/75	1/90
1/50	1/60
1/25	1/30

Manual Mode (Fixed Shutter)

Manual Mode opens the iris completely with a fixed gain. Users can select a suitable shutter speed according to the environmental luminance. The fixed shutter speed is selected from 1 to 1/10000 sec (NTSC) and 1/1.5 to 1/10000 sec (PAL). Users should select suitable shutter speed according to the environmental luminance. See following table, which shows all the options.

Manual Mode - Fixed Shutter Speeds	
PAL	NTSC
1/10000	1/10000
1/3500	1/3000
1/2500	1/2000
1/1250	1/1000
1/600	1/725
1/425	1/500
1/300	1/350
1/215	1/250
1/150	1/180
1/120	1/120
1/100	1/100
1/75	1/90
1/50	1/60
1/25	1/30
1/12	1/15
1/6	1/8
1/3	1/4
1/1.5	1/2
	1

Gain

A nominal video signal level is usually 1 volt peak-to-peak for composite video, 0.7 volts for component or RGB video, or 0.3 volts for the chrominance subsection, at which level a fully saturated picture is transmitted to the acceptor. However, for cases where the video signal is attenuated, a low-noise, high-gain analog amplifier is built into quality video processing equipment. This amplifier provides video gain control whereby the video signal can be boosted or reduced. Dark pictures resulting from low level lighting are easily adjusted.

The *Gain* drop-down menu enables controlling the video gain from *Off* or in steps from 1 to 9.

7.5.2 White Balance

Shown below is the drop-down menu for controlling the camera's white balance (color balance).

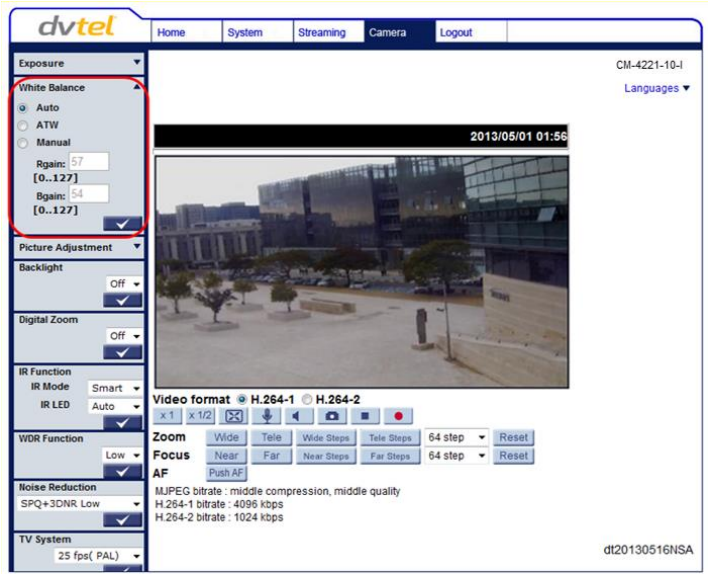


Figure 89: Camera Settings Screen – White Balance

A camera needs to find a reference color temperature as a way of measuring the quality of a light source for calculating all other colors. The unit for measuring this ratio is in Kelvin (°K) degrees. You can select one of the White Balance control modes according to the operating environment. The table below shows the color temperature of some light sources for reference.

Light Sources	Color Temperature in K
Cloudy Sky	6,000 to 8,000
Noon Sun and Clear Sky	6,500
Household Lighting	2,500 to 3,000
75-watt Bulb	2,820
Candle Flame	1,200 to 1,500

Three white balance modes are available:

- *Auto* – The Auto Balance White mode computes the white balance value output using color information from the entire screen. It is suitable for an environment with a light source color temperature in the range of approximately 2,700 ~ 7,500K.
- *ATW (Auto Tracking White Balance)* – The Auto Tracking White Balance function automatically adjusts the white balance in a scene while temperature color is changing. The ATW Mode is suitable for an environment with a light source color temperature in the range of approximately 2500 ~ 10,000K.

- *Manual* – In this mode, you can manually change the white balance value. You can select a number between 0 – 127 for either/both Rgain and Bgain to increase the red and/or blue luminance. Press <√> to confirm the new setting.

7.5.3 Picture Adjustment

Adjustment of some qualities of the video is made possible by selecting Picture Adjustment in the **Camera** tab. Brightness, Sharpness, Contrast, Saturation and Hue may all be adjusted via drop-down menus from this window, as shown below.

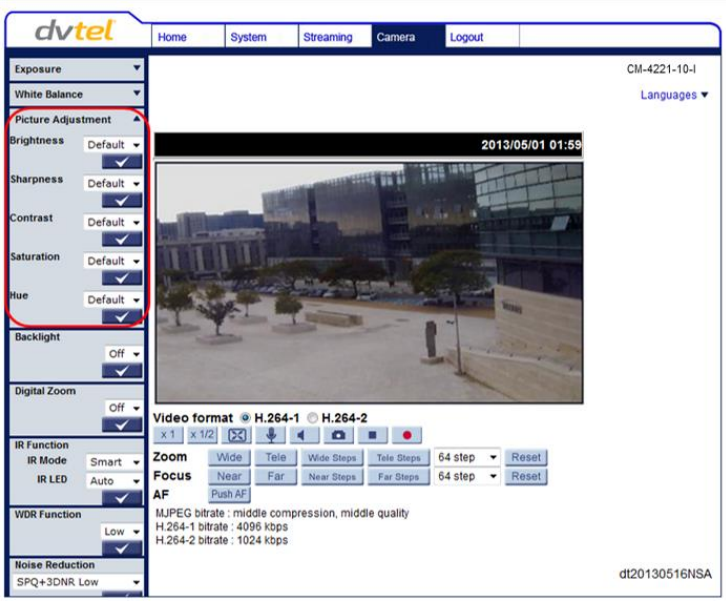


Figure 90: Camera Settings Screen – Picture Adjustment

7.5.3.1 Brightness

You can adjust the image's brightness by adjusting this parameter. Select from the range between -12 to +13. To increase video brightness, select a larger number. Press <√> to confirm the new setting

7.5.3.2 Sharpness

Increasing the sharpness level can make the image look sharper, especially enhancing the object's edge. Select from the range between 0 to +15. Press <√> to confirm the new setting.

7.5.3.3 Contrast

Camera image contrast level is adjustable. Select from a range of -6 to +19. Press <√> to confirm the new setting

7.5.3.4 Saturation

Camera image saturation level is adjustable. Select from a range of -6 to +19. Press <√> to confirm the new setting.

7.5.3.5 Hue

Camera image hue level is adjustable: select from a range of -12 to +13. Press <√> to confirm the new setting.

7.5.4 Backlight

The Backlight Compensation function prevents the center object from being too dark in surroundings where excessive light is behind the center object. Select *On* or *Off*. Press <√> to confirm the new setting.

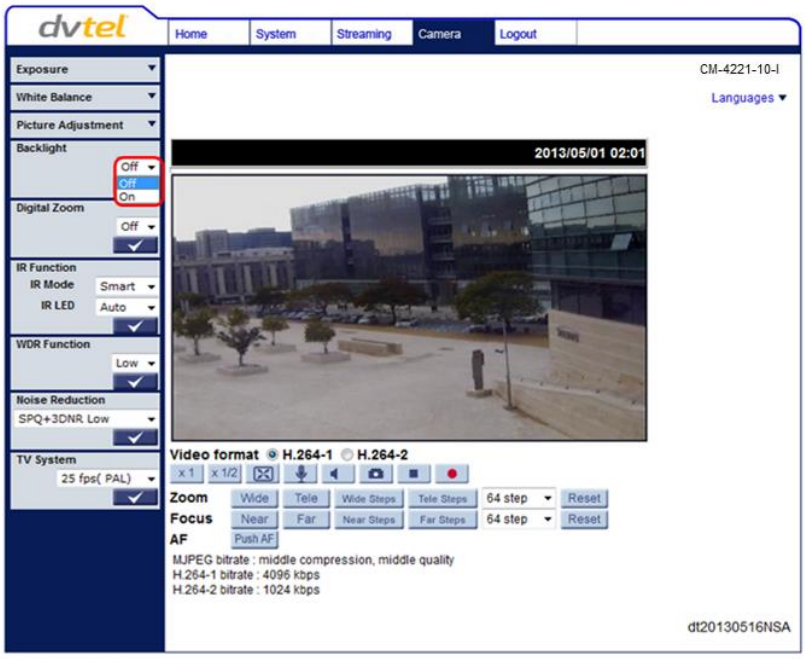


Figure 91: Camera Settings Screen – Backlight

7.5.5 Digital Zoom

The camera's digital zoom is adjustable from x2 to x8. Select the desired zoom or *Off*. Press <√> to confirm the new setting.

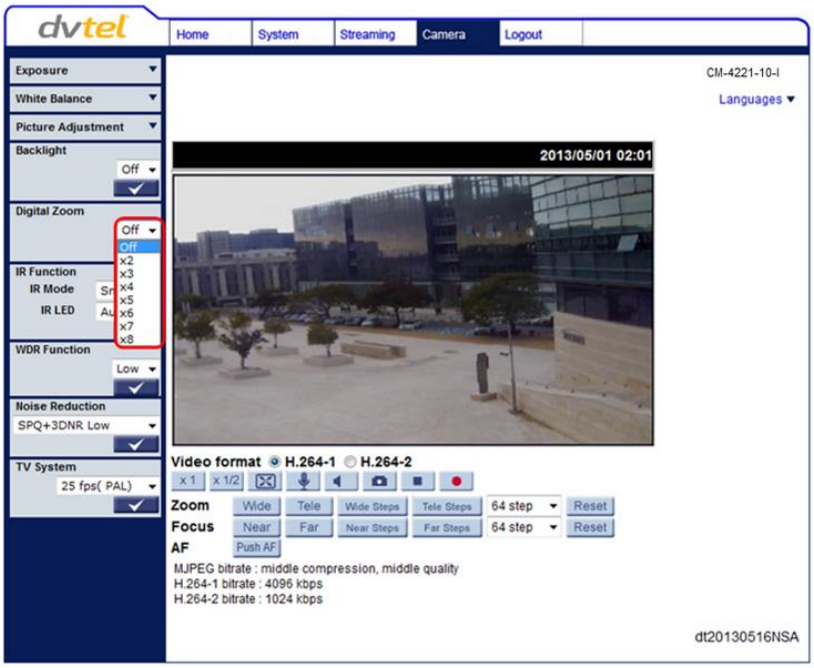


Figure 92: Camera Settings Screen – Digital Zoom

7.5.6 IR Function

The IR Function setting activates two functions:

- On the CM-3211/4221-10-I and CM-3211/4221-11-I cameras, it activates the IR LED illuminator for use in low-light conditions or at night.
- On all other cameras, it activates *IR mode*, which is the IR Cut (IRC) filter for electronic day/night operation.

IR LED Illuminator

This setting is used in low-light conditions or at night. IR LED lights are turned *On* or *Off*, depending on the light sensor. The default mode is *Auto.* Two settings are available:

- *Auto* – The light sensor operates automatically.
- *Off* – The IR light is always off.

Press <√> to confirm the new setting.

Note:
The IR LED function is available only on CM-3211/4221-10-I and CM-3211/4221-11-I.

IR Mode

The day/night IRC switching mechanism operates according to the ambient light level rather than activation of the IR LED mode. The *IR Mode* drop-down menu enables you to select from *Auto/On/Off/Smart* modes. The default mode is *Smart*. Following is an explanation of the four settings:

- *Auto Mode* – The camera converts from Day mode (color) to Night mode (monochrome) automatically at nighttime or in low light conditions. When there is sufficient light, the camera converts automatically from Night mode to Day mode.
- *On* – Activates IR mode (puts camera into monochrome/Night mode).
- *Off* – Deactivates IR mode (puts camera into color/Day mode).
- *Smart* – Smart mode enhances monochrome/Night mode stability when IR illumination is dominant and keeps the camera from switching between Day and Night modes. In this mode, the IR Cut filter is on (i.e. monochrome/Night mode) when the IR LED illuminator also is activated. This prevents the camera from returning to color/Day mode.

Press <√> to confirm the new setting.

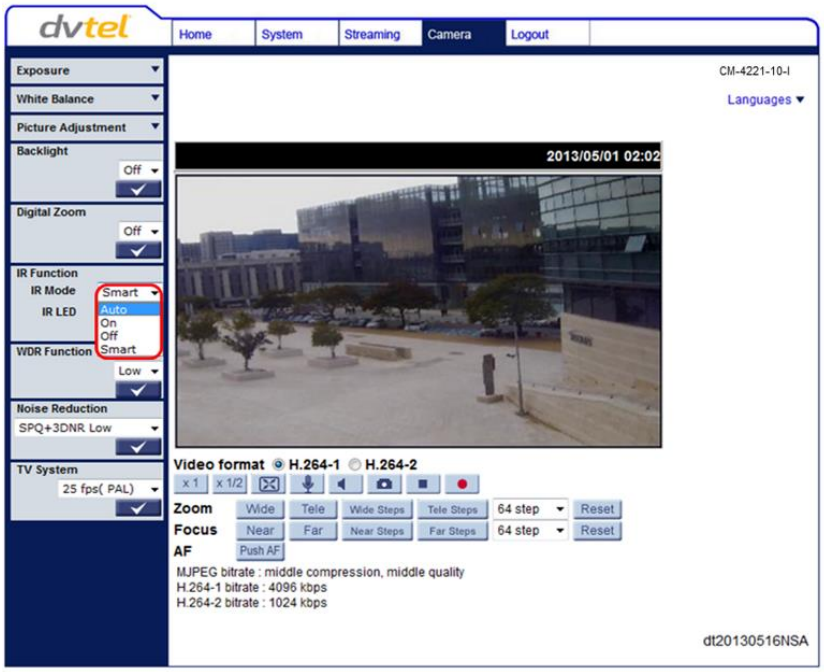


Figure 93: Camera Settings Screen – IR Function

7.5.7 WDR Function

The Wide Dynamic Range (WDR) function resolves high contrast or changing light issues in order to enhance the video display. The WDR is adjustable from *Low, Mid* to *Hi*. A higher level of WDR represents wider dynamic range, so that the IP camera can capture a greater scale of brightness. Press <√> to confirm the new setting.

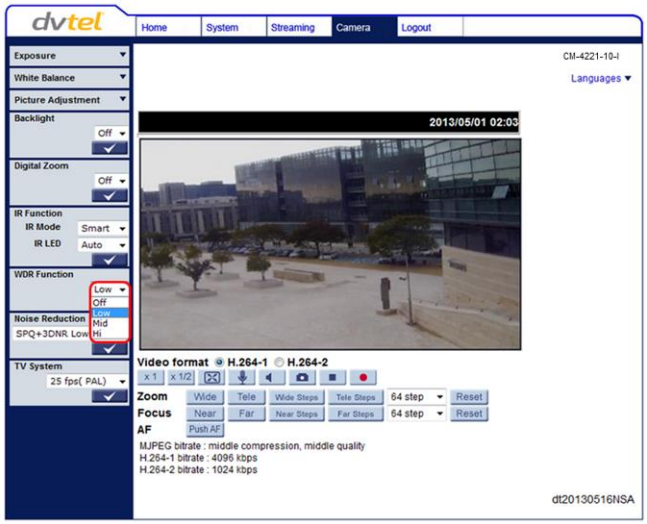


Figure 94: Camera Settings Screen – WDR Function

7.5.8 Noise Reduction

Different level options for 3D Noise Reduction (3DNR) include *Low, Mid* and *High*. A higher level of 3DNR generates relatively enhanced noise reduction.

The proprietary Smart Picture Quality (SPQ) video processing method can drastically minimize motion blur and provides clear images even in low-light environment. The combination of SPQ and 3DNR at different levels further yields exceptional video performance in various conditions.

The Noise Reduction function reduces image noise/snow, enabling the IP camera to deliver clearer images in low-light conditions. The Noise Reduction is adjustable from *3DNR Low, 3DNR Mid, 3DNR Hi, SPQ, SPQ + 3DNR Low, SPQ + 3DNR Mid,* to *SPQ + 3DNR Hi.*

Press <√> to confirm the new setting.

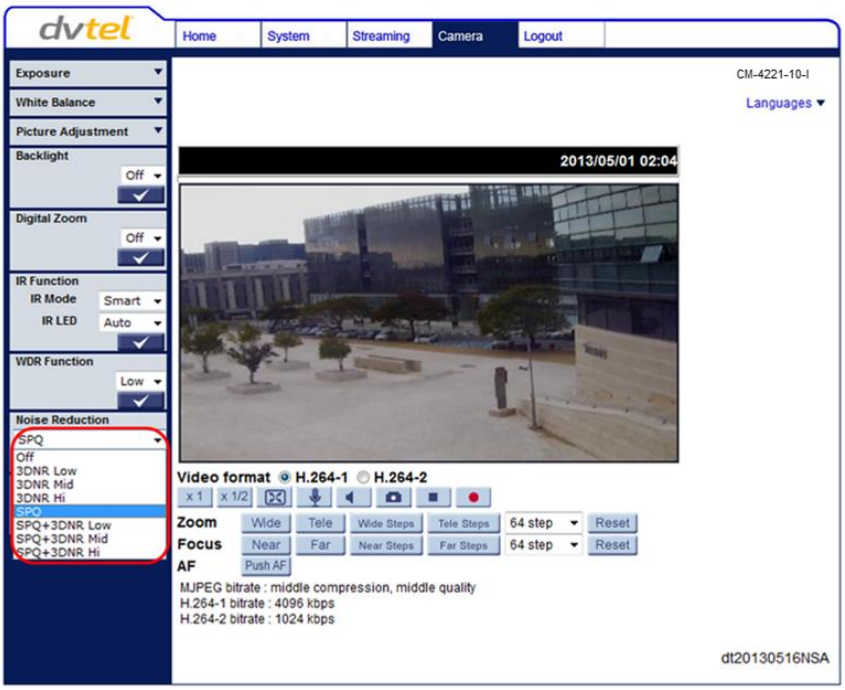


Figure 95: Camera Settings Screen – Noise Reduction

7.5.9 TV System

Select the video format that matches your TV system: *25 fps (PAL)* or *30 fps (NTSC).* Press <v> to confirm the new setting.

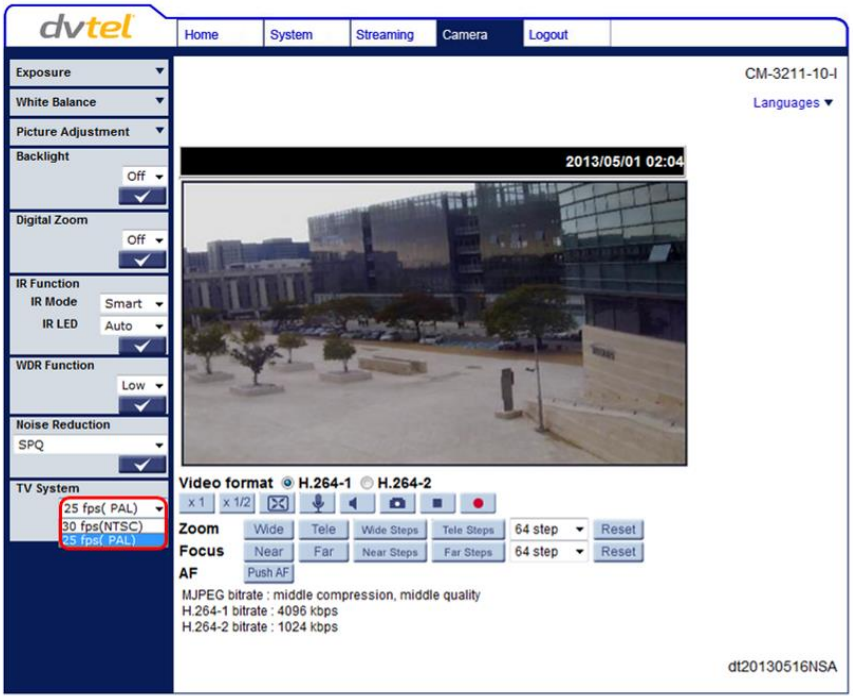


Figure 96: Camera Settings Screen – TV System

Note:
After changing the video format, the camera restarts automatically.

7.6 Logout

Selecting the **Logout** tab in the navigation bar closes the session. The following message appears:

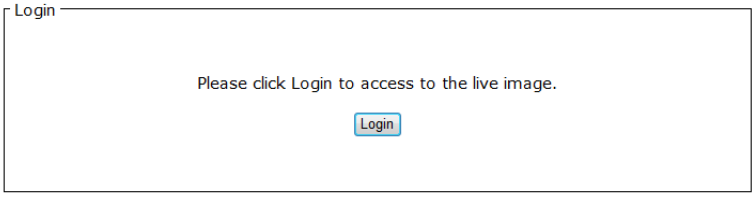


Figure 97: Login Message

Upon clicking **Login,** the **Login** window opens.

Windows Security
The server 10.70.20.42 at QuasarHDIPCamera requires a username and password.
Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).
Admin
Password
Remember my credentials
OK
Cancel

Figure 98: Login Window

8 Appendices

- Technical Specifications
- Device Search Software
- Internet Security Settings
- Install UPnP Components
- Deleting Existing DCViewer
- Deleting Temporary Internet Files
- Connecting Leads to a Spring Clamp Terminal Block
- Mounting Accessories

A.1. Technical Specifications

Camera				
Image Sensor		1/3” 1280 x 1024 CMOS		
Effective Pixels	CM-3211-xx	1280 x 720 (H x V)		
	CM-4221-xx	1920 x 1080 (H x V)		
Shutter Speed		1.0 to 1/10,000 (auto)		
Sensitivity		0.2 Lux @F1.2 in color mode; 0.02 Lux in night mode		
Enclosure		Tamper-resistant surface mount plastic case		
Lens				
Lens Type		CM-3211/4221-00	CM-3211/4221-01	CM-3211/4221-10 CM-3211/4221-10-I CM-3211/4221-11 CM-3211/4221-11-I
		Varifocal F1.2/f=2.7-9mm	Varifocal F1.2/f=2.7-9mm	Motorized F1.2/f=2.7-9mm
Video				
Video Resolution		Full HD 1080p (1920 x 1080)/SXGA (1280 x 1024)/HD 720p/D1/CIF/ VGA/XGA/SVGA		
Video Streaming		Simultaneous H.264 1080p (25/30 fps) + H.264 D1 (25/30 fps)		
Operation				
Image Setting	Brightness	Manual		
	Exposure	Auto-iris, Auto/Fixed Shutter		
	Sharpness	Manual		
	Contrast	Manual/Auto/ATW		
	Hue	Manual		
	Backlight Compensation	On/Off		
	Digital Zoom	Supported (x2 to x8)		
	WDR	On/Off + 3 levels		
	3DNR	On/Off + 3 levels (with Latitude), On/Off + 6 levels (without Latitude)		
	Privacy Mask (Video Mask)	Web interface: On/Off. Up to five embedded web interfaces are supported in the streaming video output, but are not supported by Latitude. In the Latitude interface, the Privacy Mask is independent of the camera’s on-screen display and is not embedded.		
	IR Function	Day/Night (Auto/On/Off/Smart)		
Audio	Two-way Audio	Line out/Line in		
	Compression	G.711/G.726 (not supported by Latitude)		
Alarm	Input	5V 10kΩ pull up		
	Output	Photo Relay Output 300V DC/AC		
Event Notification		HTTP, FTP, SMTP		
Languages		English, German, French, Italian, Simplified Chinese, Traditional Chinese, Russian, and Korean		
MicroSD/SDHC Card Recording		Up to 32GB microSD/SDHC card (card not included)		

Analytics		
Motion Detection		On/Off, plus sampling pixel interval, detection level, sensitivity level, and time interval settings.
Regions of Interest		Web interface: Configurable up to 10 ROI masks. Latitude interface: Configurable up to six ROI masks.
Motion Metadata		Streaming and recorded video includes per frame level motion metadata. Motion metadata is archive searchable by ROI via the Latitude ControlCenter user interface.
Triggered Actions		Notifications, On-Event Recording and Relay Output Command. Includes configurable alarms and broad range of recording on detection of video and snapshots.
Tampering Alarm		On/Off, plus duration, on-event notification, recording to SD card, and more are supported as events in Latitude.
IR Illuminator (CM-3211/4221-10-I/11-I)		
Working Distance		15.24 meters (50 ft.)
Wavelength		850nm
LEDs		24
Network		
Interface		10/100Mbps Ethernet, Auto-sensing, Full/Half-Duplex
Protocol		IPv4/v6, TCP/IP, UDP, RTP, RTSP, HTTP, HTTPS, ICMP, FTP, SMTP, DHCP, PPPoE, UPnP, IGMP, SNMP, QoS, and ONVIF
Password Levels		User and Administrator
Security		HTTPS, IP Filter, IEEE 802.1x
Internet Browser		Internet Explorer (IE 7, 8, and 9)
User Accounts		20
Mechanical		
Connectors	Power	3-pin terminal block
	Ethernet	RJ45
	Audio	4-pin terminal block with audio input and audio output
	Alarm	4-pin terminal block with 2-pin alarm input and 2-pin relay output
	Analog Video	1.0V p-p/75Ω, BNC (continuously enabled)
LED Indicator		Power, Link, ACT
Weatherproof Standard		IP66 on CM-3211/4221-01, CM-3211/4221-11, and CM-3211/4221-11-I
Mechanical IR Cut Filter		On CM-3211/4221-01, CM-3211/4221-11, and CM-3211/4221-11-I

<table>
<tr><td colspan="8">Physical</td></tr>
<tr><td colspan="2" rowspan="2">Dimensions</td><td>CM-3211/4221-00</td><td>CM-3211/4221-01</td><td colspan="4">CM-3211/4221-1x</td></tr>
<tr><td>149 x 131 mm
(5.9 x 5.2 in.)</td><td>151 x 130 mm
(5.9 x 5.1 in.)</td><td colspan="4">151 x 130 mm
(5.9 x 5.1 in.)</td></tr>
<tr><td colspan="2">Weight</td><td>0.7 kg (1.5 lbs.)</td><td>0.8 kg (1.8 lbs.)</td><td colspan="4">0.8 kg (1.8 lbs.)</td></tr>
<tr><td colspan="8">Electrical</td></tr>
<tr><td colspan="2" rowspan="2">Power Consumption (Watts)</td><td rowspan="2">CM-3211/4221-00</td><td rowspan="2">CM-3211/4221-01</td><td colspan="4">CM-3211/4221-1x</td></tr>
<tr><td>-10</td><td>-10-I</td><td>-11</td><td>-11-I</td></tr>
<tr><td colspan="2">Power Source</td><td>5W</td><td>12W
(w/ heater and fan)</td><td>15.6</td><td>18.6</td><td>15.6</td><td>18.6</td></tr>
<tr><td colspan="8">Environmental</td></tr>
<tr><td colspan="2" rowspan="2">Operating Temperature</td><td>CM-3211/4221-00</td><td>CM-3211/4221-01</td><td colspan="4">CM-3211/4221-1x</td></tr>
<tr><td>-10° to 50°C
(-14° to 122°F)</td><td>@12VDC:
-30°to 50°C
(-22°F to 122°F)
w/ heater and fan</td><td colspan="4">@24VAC:
-35° to 50°C
(-31° to 122°F)
w/ heater and fan</td></tr>
<tr><td colspan="2">Humidity</td><td colspan="6">10-90% non-condensing</td></tr>
<tr><td colspan="8">General</td></tr>
<tr><td rowspan="2">Regulatory</td><td>US</td><td colspan="6">FCC Part 15 (Subpart B, Class A) UL</td></tr>
<tr><td>Europe</td><td colspan="6">CE-marked, EN55022-1998 Class A, EN55024, RoHS</td></tr>
<tr><td colspan="2">Warranty</td><td colspan="6">Lifetime covering parts</td></tr>
</table>

A.2. Device Search Software

A.2.1 Initial Camera Configuration

To perform the initial camera configuration:

1. Unpack the camera. Rotate and remove the protective cover.
2. Remove the PE cloth sheet and lens cap. Attach the dome cover to the body.
3. Insert the RJ45 plug at the end of the network cable into the network port of the camera.
4. Do one of the following:
   - Copy and run the `devicesearch.exe` from the included CD.

     Note:
     Device Search is an alternative software to DNA. Either of these programs may be used. Both are supplied on the included CD.
   - From the Latitude Sidebar, run the Unified Configurator by selecting *Applications* > *Device Configuration Tool* and then on the Unified Configurator screen, click **DVTEL HD Series**.
5. In the Device Search application, click **Device Search** and do the following:
   a. In the search results, click on the camera to select it.
   b. Right-click and select from the shortcut menu **Network Setup**.

Figure 99: Device Search Application

   c. In the dialog that appears, select **Static IP**.
   d. Enter the *IP Address, Gateway* and *Netmask* (network mask) as needed and click **OK**.
6. Disconnect the Ethernet cable. The camera is ready for deployment in a site installation (mounting).

Note:
The camera can be connected to a PC for bench installation via an Ethernet cross-cable.

Note:
The camera default IP Address and the subnet mask IP Address are automatically supplied by the DHCP server.

Tip:
A camera setup adapter, such as Veracity Pinpoint, can be used to connect a laptop directly to the camera when using PoE.

A.2.2 Searching and Accessing the Camera with Device Search

Device Search provides a central location for listing all the DVTEL CM, CF and CP camera models accessible over the network. Once listed, each camera can be right-clicked to access and change the network settings.

Once the network settings are changed, a new search will relist the units. The units may then be configured via the web interface.

If DVTEL Latitude is being used, configure the unit with a static IP address rather than with DHCP. This ensures that the IP address will not automatically change in the future and interfere with configurations and communication.

The camera must be made accessible for the network's addressing. For initial access to the camera, do either of the following and search and configure the camera's network settings via Device Search:

- In Latitude, the Device Configuration Tool (Unified Configurator) can be accessed from the Applications menu, if AdminCenter is available. Click the **DVTEL HD Series** button.
- Run devicesearch.exe, which can be found in the Device Search folder in the supplied CD.

Note:
Device Search is an alternative software to DNA. Either of these programs may be used. They are supplied in the included CD.

A.2.3 Configuring Communication Settings of a Quasar Camera

1. Connect the camera to the network on the same VLAN/LAN as the workstation.
2. If the network supports the default, open Device Search by doing one of the following:

   a. Access the Device Configuration Tool (Unified Configurator) from the Applications menu, if the AdminCenter in Latitude is available. Click the **DVTEL HD Series** button.

   b. Run `devicesearch.exe` which can be found in the Device Search folder in the supplied CD.

Note:
Device Search is an alternative software to DNA. Either of these programs may be used. They are supplied on the included CD.

3. In the Device Search application, click the **Device Search** button. See Figure 99: Device Search Application.
4. If the Windows Firewall is enabled, a security alert window will pop up. Do the following:
   a. Click **Unblock** to continue. Latitude users should consult the Latitude Installation Instructions on disabling the Windows Firewall.

Windows Security Alert
To help protect your computer, Windows Firewall has blocked some features of this program.
Do you want to keep blocking this program?
Name: DeviceSearch
Publisher: Unknown
Keep Blocking
Unblock
Ask Me Later
Windows Firewall has blocked this program from accepting connections from the Internet or a network. If you recognize the program or trust the publisher, you can unblock it. When should I unblock a program?

Figure 100: Windows Security Alert

   b) Click **Device Search** again. All the discovered IP devices will be listed in the page, as shown in the figure below. The camera's default IP address is automatically set by the DHCP server.

5. Right-click on the camera whose network property is to be changed. From the menu that opens, select **Network Setup**. The **Network Setup** dialog is displayed.

> **Tip:**
> Record the camera's MAC address for future reference.

6. To access **Device Search**, do one of the following:
   a) For DHCP (not supported by Latitude):
      i) Select **DHCP**. Do not use for Latitude.
      ii) Click **Apply**. When prompted with instructions to search again after one minute, click OK.
      iii) After one minute, click **Device Search**.
   b) For Static IP (recommended for Latitude users):
      i) Select **Static IP** (preferable for security and Latitude users). In the IP Address, Gateway, and Netmask, enter the respective LAN/VLAN (optional DNS) values.
      ii) Click **Apply**. When prompted with instructions to search again after one minute, click **OK**.
      iii) After one minute, click **Device Search**. The communication settings should now be changed and ready to install the camera on the network. Access it either via the browser-based viewer or Latitude NVMS.

7. Right-click and select **Browse** to directly access the camera via a web browser. The default web browser opens and requests access to the camera IP address.

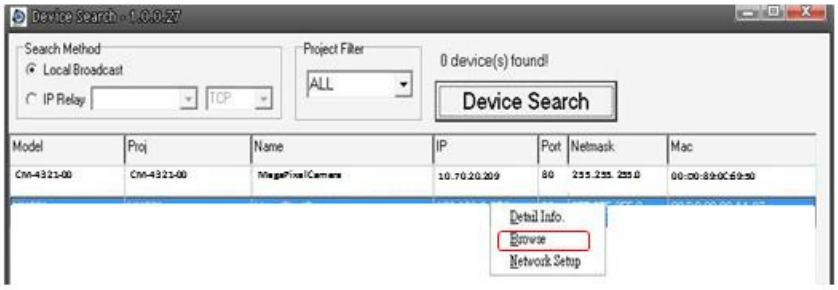


Figure 101: Device Search Application – Select Browse

8. When the web browser contacts the camera IP, do the following:

   a) Log in using the default user name *Admin* and password *1234*.

> **Note:**
> ID and password are case-sensitive.

> **Note:**
> It is strongly advised that administrator's password be altered for security reasons.

   b) If the Information Bar (just below the URL bar) prompts for permission to install the ActiveX Control for displaying video in the browser (see the figure below), right-click on the Information Bar. Select Install ActiveX Control to allow the installation.

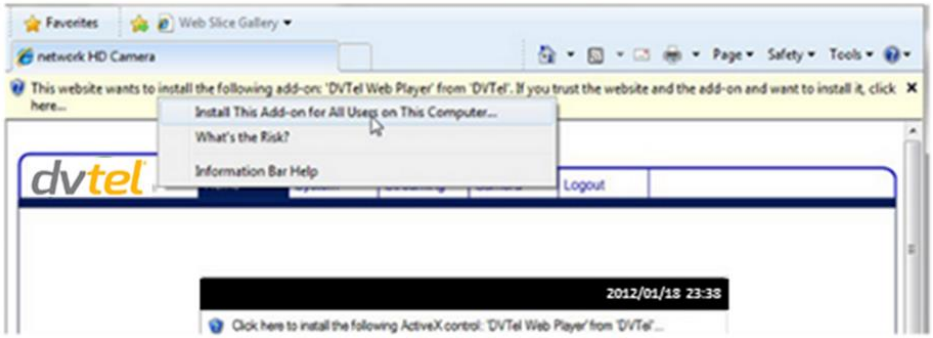

Favorites
Web Slice Gallery
network HD Camera
Page
Safety
Tools
This website wants to install the following add-on: 'DVTel Web Player' from 'DVTel'. If you trust the website and the add-on and want to install it, click here...
Install This Add-on for All Users on This Computer...
What's the Risk?
Information Bar Help
dvtel
Logout
2012/01/18 23:38
Click here to install the following ActiveX control: 'DVTel Web Player' from 'DVTel'...

Figure 102: Device Search Application – Select Install ActiveX Control

9. If a security warning window prompt appears, click **Install**.

Internet Explorer - Security Warning
Do you want to install this software?
Name: DVTel Web Player
Publisher: DVTel
More options
Install
Don't Install
While files from the Internet can be useful, this file type can potentially harm your computer. Only install software from publishers you trust. What's the risk?

Figure 103: Security Warning Window

10. If the wizard appears for installing the component application DCViewer, follow the instructions to complete the installation.

> **Note:**
> If the password is changed and DVTEL Latitude AdminCenter Discovery feature is in use, deselect all other proprietary types. Select DVTEL HD Series so that the new password can be configured in the Discovery tab settings.

Additionally, you can change the camera's network property (either DHCP or Static IP) directly in the device finding list. Refer to the following section for changing the camera's network property.

A.3. Internet Security Settings

If ActiveX control installation is blocked, either set Internet security level to default or change ActiveX controls and plug-in settings.

To set the default Internet security level:

1. Start Internet Explorer (IE).
2. From the Command Bar toolbar, select Tools and select Internet Options from the menu that appears.

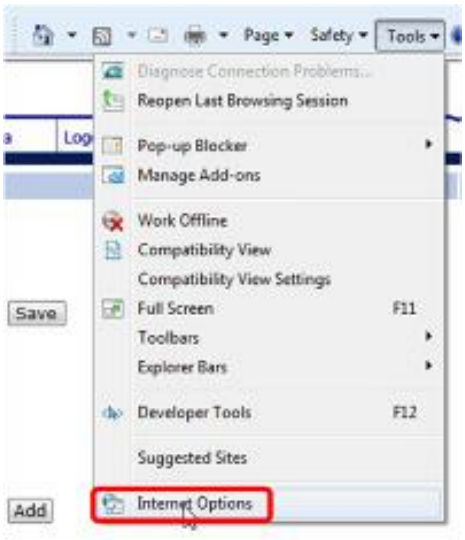


Figure 104: Command Bar Toolbar – Select Internet Options

3. In the Internet Options window that appears, select the Security tab.
4. Select

in Select a zone to view or change security settings.
5. If the settings are not defined as default, select Default Level and move the *Allowed* levels for this zone slider to *Medium-high* and select **OK**.

Figure 105: Internet Options Screen

6. Close all browsers and reopen so that the settings take effect.

ActiveX Controls and Plug-in Settings

To create a custom level:

1. Start Internet Explorer (IE).
2. From the Command Bar toolbar, select **Tools** and select *Internet Options* from the menu that appears.

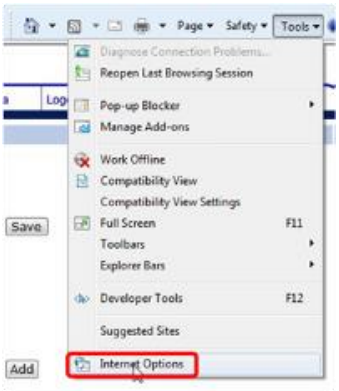


Figure 106: Command Bar Toolbar – Internet Options

3. In the **Internet Options** window that appears, select the **Security** tab.
4. If not already selected, select

, then select *Custom Level*.
5. In the dialog that appears, under **ActiveX controls and plug-ins** set ALL the following options (listed below) to **Enable** or **Prompt**:
   - Automatic prompting for ActiveX controls
   - Binary and script behaviors
   - Download signed ActiveX controls
   - Download using ActiveX controls
   - Initialize and script ActiveX not marked as safe
   - Run ActiveX controls and plug-ins
   - Script ActiveX controls marked safe for scripting

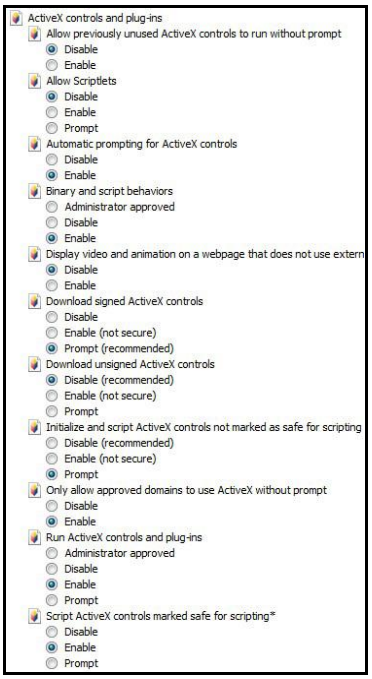
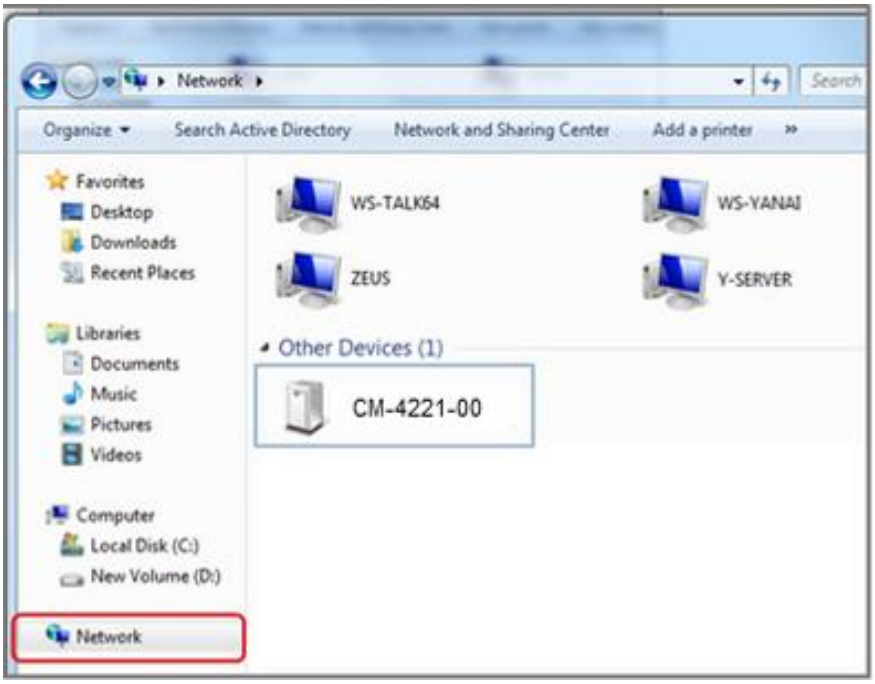


Figure 107: Schedule Screen

6. Click **OK** to accept the settings and close the **Security** screen.
7. Click **OK** to close the **Internet Options** screen.
8. Close the browser window and restart IE again to access the camera.

A.4. Install UPnP Components

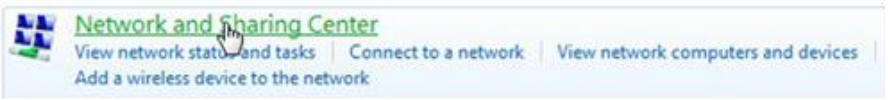
Follow the instructions below to enable UPnP so that the camera can be discovered and displayed in Network locations under *Other Devices*:



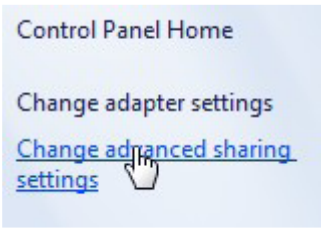
To enable UPnP discovery in Windows 7 and Windows 8:

1. Click (Start) and select *Control Panel*.
2. Click on *Network and Internet*.

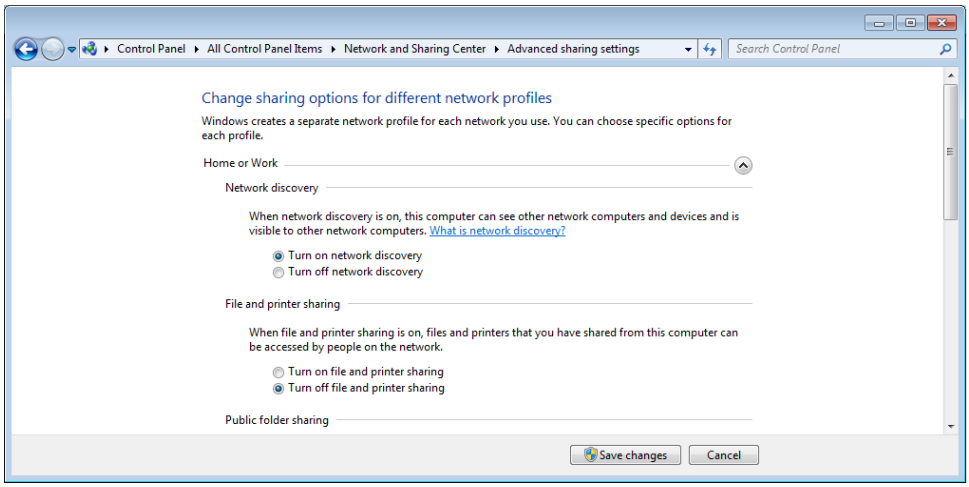
3. Click on *Network and Sharing Center*.


Network and Sharing Center
View network status and tasks
Connect to a network
View network computers and devices
Add a wireless device to the network

4. Click *Change advanced sharing settings*.



5. Expand the Home or Work node, select *Turn on network discovery.*

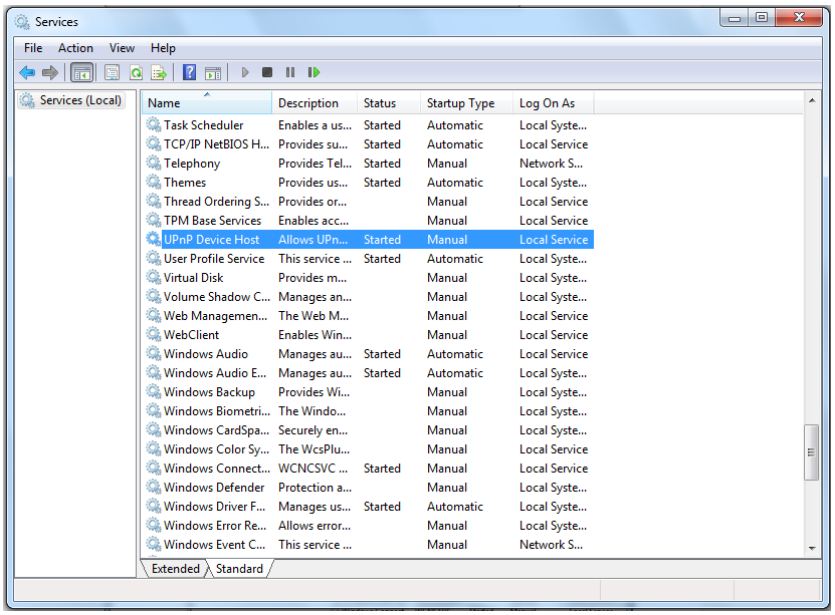

Control Panel ▸ All Control Panel Items ▸ Network and Sharing Center ▸ Advanced sharing settings
Search Control Panel
Change sharing options for different network profiles
Windows creates a separate network profile for each network you use. You can choose specific options for each profile.
Home or Work
Network discovery
When network discovery is on, this computer can see other network computers and devices and is visible to other network computers. What is network discovery?
Turn on network discovery
Turn off network discovery
File and printer sharing
When file and printer sharing is on, files and printers that you have shared from this computer can be accessed by people on the network.
Turn on file and printer sharing
Turn off file and printer sharing
Public folder sharing
Save changes
Cancel

6. Click **Save Changes**.

> **Note:**
> Network discovery requires that the DNS Client, Function Discovery Resource Publication, SSDP Discovery, and UPnP Device Host services are started, that network discovery is allowed to communicate through Windows Firewall, and that other firewalls are not interfering with network discovery.

To check that the UPnP Device Host services are running:

1. Click (Start) and type in the Search programs and files field **services.msc** and then select **services.msc** from the displayed Programs. The **Services manager** dialog box appears.


Services
File Action View Help
Services (Local)
Name Description Status Startup Type Log On As
Task Scheduler Enables a us... Started Automatic Local Syste...
TCP/IP NetBIOS H... Provides su... Started Automatic Local Service
Telephony Provides Tel... Started Manual Network S...
Themes Provides us... Started Automatic Local Syste...
Thread Ordering S... Provides or... Manual Local Service
TPM Base Services Enables acc... Manual Local Service
UPnP Device Host Allows UPn... Started Manual Local Service
User Profile Service This service ... Started Automatic Local Syste...
Virtual Disk Provides m... Manual Local Syste...
Volume Shadow C... Manages an... Manual Local Syste...
Web Managemen... The Web M... Manual Local Service
WebClient Enables Win... Manual Local Service
Windows Audio Manages au... Started Automatic Local Service
Windows Audio E... Manages au... Started Automatic Local Syste...
Windows Backup Provides Wi... Manual Local Syste...
Windows Biometri... The Windo... Manual Local Syste...
Windows CardSpa... Securely en... Manual Local Syste...
Windows Color Sy... The WcsPlu... Manual Local Service
Windows Connect... WCNCSVC ... Started Manual Local Service
Windows Defender Protection a... Manual Local Syste...
Windows Driver F... Manages us... Started Automatic Local Syste...
Windows Error Re... Allows error... Manual Local Syste...
Windows Event C... This service ... Manual Network S...
Extended Standard

2. In the **Services manager** dialog box, scroll down the list to *UPnP Device Host* and verify that it shows the status **Started**. If **Started** is not displayed, right-click and select **Start** from the shortcut menu.

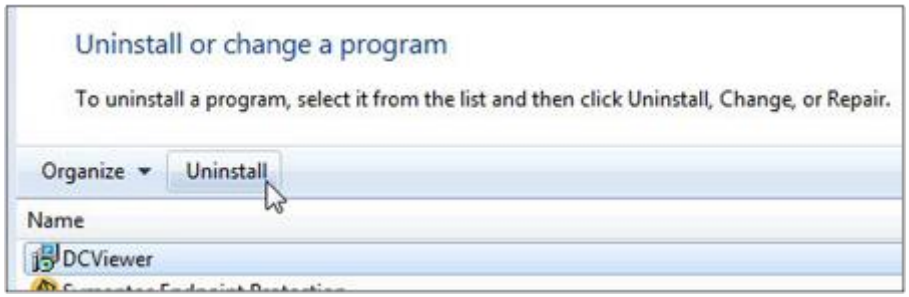
A.5. Deleting the Existing DCViewer

Users who have previously installed the DCViewer in the PC should first delete the existing DCViewer from the PC before accessing the camera.

To delete a legacy DCViewer:

1. Click **Start** and select Control Panel.
2. In the Control Panel, click **Uninstall a program**.

3. From the installed program list, select **DCViewer** and then, on the banner bar, click **Uninstall**.


Uninstall or change a program
To uninstall a program, select it from the list and then click Uninstall, Change, or Repair.
Organize
Uninstall
Name
DCViewer

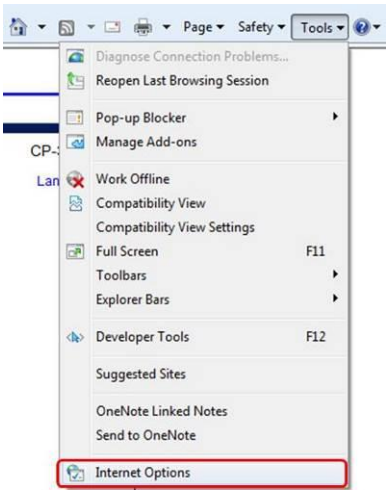
4. If prompted to confirm the Uninstall, click **Yes**.

A.6. Deleting Temporary Internet Files

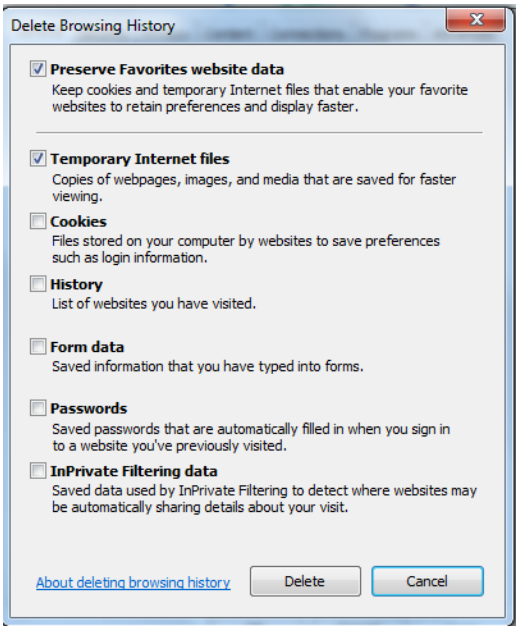
To improve browser performance, it is recommended to clean up all of the temporary Internet files.

To delete temporary Internet files:

1. In Internet Explorer (IE), from the Command Bar toolbar, click **Tools** and select *Internet Options* from the menu that appears.



2. In the **General** tab in the *Internet Options* dialog box, click **Delete**.
3. In the **Delete Browser History** dialog box that appears, select Temporary Internet files. Deselect *Cookies and History* to keep this data. Then click **Delete**.


Delete Browsing History
Preserve Favorites website data
Keep cookies and temporary Internet files that enable your favorite websites to retain preferences and display faster.
Temporary Internet files
Copies of webpages, images, and media that are saved for faster viewing.
Cookies
Files stored on your computer by websites to save preferences such as login information.
History
List of websites you have visited.
Form data
Saved information that you have typed into forms.
Passwords
Saved passwords that are automatically filled in when you sign in to a website you've previously visited.
InPrivate Filtering data
Saved data used by InPrivate Filtering to detect where websites may be automatically sharing details about your visit.
About deleting browsing history
Delete
Cancel

A.7. Connecting Leads to a Spring Clamp Terminal Block

The unit is delivered with two terminal block connectors. The connectors enable you to connect wires for either the Relay Output or Alarm Input and then connect them to the unit.

Figure 108: Spring Clamp Terminal Block

To connect a wire to the spring clamp terminal block:

1. Strip the insulation form the end of each wire that is to be connected to the terminal block. Approximately 1 cm (2.54”) of wire should be exposed.
2. With a small screwdriver, press in and hold the orange spring clamp button next to the female outlet where the wire will be inserted.
3. Insert the stripped end of the wire into the female outlet.
4. Release the orange spring clamp button.

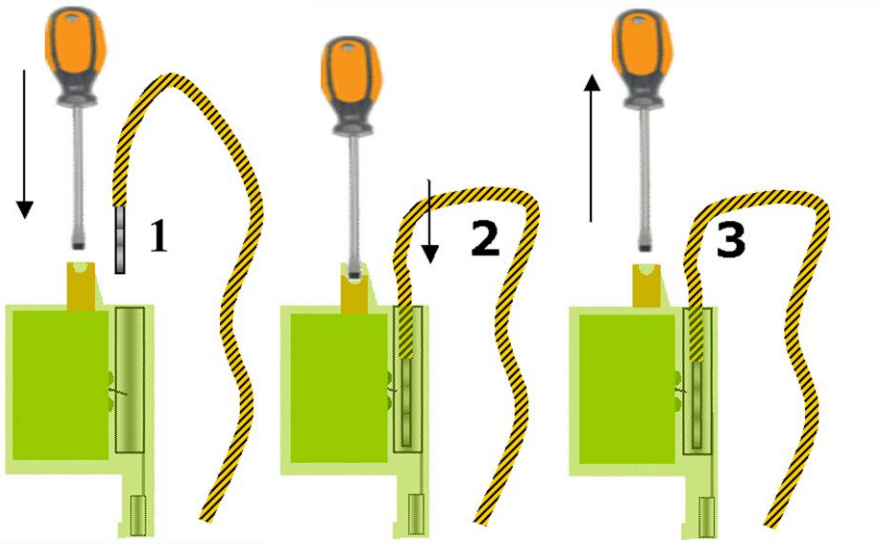


Figure 109: Connecting a Wire to a Terminal Block

A.8. Mounting Accessories

The following mounting accessories are available from DVTEL for installation of your Quasar CM-3211/4221 Series Compact Fixed Dome IP Camera. For more information on available options, contact your DVTEL sales representative or visit www.DVTEL.com to request details on where to get the accessories you need.

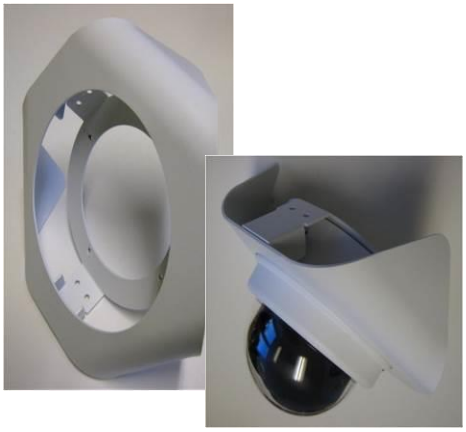
Image	Name	Description
	CM-RCSD-0	CM Series Mini-Dome Recessed Mount
	CX-TRIA-0	CM Series Mini-Dome Corner Mount
	CM-CAPX-0	CM Series Mini-Dome Pendant Mount
	CX-ARMX-0	Short Arm Bracket

Image	Name	Description
	CX-ARMX-1	Long Arm Bracket
	CX-CRNR-0	Corner Bracket fits CX-ARMX-0 and CX-ARMX-1.
	CX-F150-1	Pendant Mounting Adapter Ring adapts all pendant cameras to common legacy 1-1/2" female pipe mounts. Fits DVTEL legacy mounts and many others.
	CX-PIPE-0	Short Pipe straight tube (9.8") for pendant mount

Image	Name	Description
	CX-PIPE-1	Long Pipe straight tube (19.7") for pendant mount.
	CX-POLE-0	Pole-Mount Bracket fits CX-ARMX-0 and CX-ARMX-1.
	CX-WLBX-0	Wall Mount Box fits CX-ARMX-0 and CX-ARMX-1.

Contacting DVTEL

DVTEL Inc. is a multiple award-winning market leader in the development and delivery of intelligent security solutions over IP networks. DVTEL provides unified solutions that leverage existing network infrastructure, while providing unmatched levels of flexibility, scalability and cost-effectiveness - all backed by superior customer support.

To contact us, write us at info@DVTEL.com, or contact your local office.

CORPORATE HEADQUARTERS **DVTEL, Inc.** 65 Challenger Road Ridgefield Park, NJ 07660 USA Tel: +1 201.368.9700 Fax: +1 201.368.2615 info@DVTEL.com	**ASIA PACIFIC REGION** **DVTEL** 111 North Bridge Road, #27-01 Peninsula Plaza Singapore 179098 Tel: +65 6389 1815 Fax: +65 6491 5660 info.apac@DVTEL.com
ANZ AND THE PACIFIC ISLANDS **DVTEL** 37 Victoria Street Henley Beach, SA 5022 Australia Tel: +61 8 8235 9211 Fax: +61 8 8235 9255 info.anz@DVTEL.com	**EMEA** **DVTEL UK Ltd.** 7 Lancaster Court Coronation Road High Wycombe HP12 3TD England Tel: +44 (0) 1494 430240 Fax: +44 (0) 1494 446928 info.uk@DVTEL.com
INDIA AND SAARC, GULF REGION **DVTEL, India Pvt., Ltd** 303 SSR Corporate Park Mathura Road Faridabad 121002 Haryana, India Tel: +91 (129) 431 5031 Fax: +91 (129) 431 5033 info.asia@DVTEL.com	**CENTRAL AND LATIN AMERICA** **DVTEL Mexico S.A.P.I. de C.V**. Felipe Villanueva No. 10 Col. Guadalupe Inn México D. F. 01020 México Tel: +52 55 5580 5618 Fax: +52 55 8503 4299 info.cala@DVTEL.com
DVTEL NORTH ASIA 2404, 24/F, World-Wide House 19 Des Voeux Road Central Hong Kong Tel: +852 3667 9295 Mobile: +852 9479 4195 info.northasia@DVTEL.com	**DVTEL 中国** **北京朝阳区西大望路甲1号 温特莱中心B座12层09** 单元 100026 电话: +86-10-8586-8836 **手机**: +86-13501266857 传真: +86-10-8586-8815 邮箱: info.china@DVTEL.com

To request the latest versions of firmware and software or to download other product-related documents, visit http://www.DVTEL.com/support. If you have obtained a login, go to our support gateway. For assistance, email us at support@DVTEL.com or phone 1-888-DVTEL77.